EXHIBIT A

COLLEGE OF MARIN

Agenda Item Details

Meeting	Aug 15, 2017 - Regular Board Meeting
Category	I. Consideration and Possible Action
Subject	8. Award of RFP 17-0726: District Wide Hardware and Software
Type	Action

The District currently utilizes a wireless lock system for installation of door hardware. RFP 17-0726 was developed to secure pricing for a period of 3 years for this equipment. In addition to the 3 years, the District has the right to have 2-1 year extensions on the contract. In addition to securing pricing the RFP also allows other CSUs, UCs, K-12 and Community Colleges to "piggyback" off this contract to allow those entities to purchases the same material. The District has built in ½ of 1% cost recovery fee into the RFP that will be charged to the vendor for each contract issued. This fee is to cover the cost of overhead for the District to administer the grant.

By utilizing this RFP, contractors can purchase directly from this pricing list with defined terms in order to lock in pricing. Also, the District can have definitive pricing for future replacement costs as units may need to be replaced for routine maintenance.

Staff recommends the approval of this RFP to SecureAll Inc. for a period of 3 years, which is applicable pursuant to the Government Procurement Code.

RFP-17-0726 Districtwide Hareware Software Project.pdf (1,619 KB)

Price List District Wide Hardware Software 17-0726.pdf (9,174 KB)

District Wide Hardware Software 17-0726.pdf (703 KB)

COLLEGE OF

MARIN

District Wide Electronic Hardware/Software
Project #17-0726

Marin Community College District

Bid Date: 2:00 p.m. Friday, August 11, 2017

NOTICE INVITING BIDS

1. Notice is hereby given that the Governing Board ("Board") of the Marin Community College District ("District"), of the County of Marin, State of California, will receive sealed bids for the **District Wide Electronic Hardware/Software Project #17- 0726,** ("Project") up to, but not later than, **2:00 p.m. Friday, August 11, 2017**, and will thereafter publicly open and read aloud the bids. All bids shall be received at the office of the **District Buyer,** College of Marin, Indian Valley Campus, 1800 Ignacio Blvd., Administrative Services Building 8, Room 130, Novato, California, 94949.

   Bid opening will occur at 2:00 p.m. on the date stated above at the College of Marin, Indian Valley Campus, 1800 Ignacio Blvd., Administrative Services Building 8, Room 130, Novato, California, 94949.

   Note: It is the responsibility of the bidder to make sure that the bid is delivered to the address listed above. Please be informed that UPS does not deliver directly to this physical address.

2. Each bid shall be completed on the Bid Proposal Form included in the Contract Documents, and must conform and be fully responsive to this invitation, the plans and specifications and all other Contract Documents. The Contract Documents are available for review at the College of Marin, Indian Valley Campus, 1800 Ignacio Blvd., Administrative Services Building 8, Room 130, Novato, California.

3. Each bid shall be accompanied by a bidder's bond executed by a surety licensed to do business in the State of California as a surety, made payable to the District, in an amount not less than ten percent (10%) of the maximum amount of the bid. The bid bond shall be given as a guarantee that the bidder to whom the contract is awarded shall execute the Contract Documents and will provide performance bonds and insurance certificates within ten (10) days after the notification of the award of the Contract.

4. The substitution of appropriate securities in lieu of retention amounts from progress payments in accordance with Public Contract Code §22300 is permitted.

5. Pursuant to Public Contract Code §4104, each bid shall include the name and location of the place of business of each subcontractor who shall perform work or service or fabricate or install work for the contactor in excess of one-half of one percent (1/2 of 1%) of the bid price. The bid shall describe the type of work to be performed by each listed subcontractor.

6. No bid may be withdrawn for a period of ninety (90) days after the date set for the opening for bids except as provided pursuant to Public Contract Code §§5100 *et seq*. **The District reserves the right to reject any and all bids and to waive any informalities or irregularities in the bidding.**

7. Minority, women, and disabled veteran contractors are encouraged to submit bids. This

bid **is not** subject to Disabled Veteran Business Enterprise requirements. The MCCD is a self-certifying District and a vendor wanting to self-certify may do so by request to the District and a form shall be provided based on the category the vendor is claiming as a Minority, small, women owned or veteran owned company as set forth by federal regulations.

8. This contract **is not** subject to a **labor** compliance program, as described in the Labor Code.

MARIN COMMUNITY COLLEGE DISTRICT
By: Greg Nelson, Vice President, College Operations

DATED: July 26, 2017

INSTRUCTIONS TO BIDDERS

Each bid submitted to the Marin Community College District ("District") for the **District Wide Electronic Hardware/Software #17-0726** shall be in accordance with the following instructions and requirements, which are part of the Contract Documents for this Project.

1. Deadline For Receipt of Proposals. Each bid shall be sealed and submitted to the District Buyer **no later than 2:00 p.m. on Friday, August 11, 2017.** The District suggests that bids be hand delivered in order to ensure their timely receipt. Any bids received after the time stated, regardless of the reason, shall be returned, unopened, to the bidder. The Buyer office is located at College of Marin, Indian Valley Campus, **1800 Ignacio Boulevard, Building 8, Room 130, Novato, California, 94949**.

2. Terms. The term of this contract shall be for a period of three (3) years with the option to renew for two (2) one year options for a total award not to exceed five (5) years.

   Escalation of pricing within terms of this agreement shall be denoted by the vendor in their proposal for consideration and shall be limited to no more than five (5) percent per year of the contract agreement with the awarded vendor.

3. Requests for Information. A bidder's failure to request clarification or interpretation of an apparent error, inconsistency or ambiguity in the Contract Documents waives that bidder's right to thereafter claim entitlement to additional compensation based upon an ambiguity, inconsistency, or error, which should have been discovered by a reasonably prudent Contractor, subject to the limitations of Public Contract Code §1104. Any questions relative to the bid shall be in writing and directed to the District Buyer at the address specified for receipt of bid proposals. These requests may be faxed to the District Buyer at (415) 883-3261. These requests shall be submitted to the District at least three (3) working days prior to the date the bid is due.

4. Bid Proposal Forms. All bid proposals shall be made on the forms provided by the District. All items on the form shall be filled out in ink. Numbers should be stated in figures, and the signatures of all individuals must be in long hand. The completed form shall be without interlineations, alterations, or erasures.

5. Execution of Forms. Each bid must give the full business address of the bidder and must be signed by the bidder or bidder's authorized representative with his or her usual signature. Bids by partnerships must furnish the full names of all partners and must be signed in the partnership name by a general partner with authority to bind the partnership in such matters. Bids by corporations must be signed with the legal name of the corporation, followed by the signature and designation of the president, secretary, or other person authorized to bind the corporation in this matter. The name of each person signing shall also be typed or printed below the signature. When requested by the District, satisfactory evidence of the authority of the officer signing on behalf of the corporation or partnership shall be furnished. A bidder's failure to properly sign required forms may result in rejection of the bid. All bids must include the bidder's contractor license number(s) and expiration

date(s).

6. Bid Security. Bid proposals shall be accompanied by a certified or cashier's check or bid bond for an amount not less than ten percent (10%) of the bid amount, payable to the District. A bid bond shall be secured from an admitted surety company, licensed in the State of California, and satisfactory to the District. The bid security shall be given as a guarantee that the bidder will enter into the Contract if awarded the work, and in the case of refusal or failure to enter into the Contract within ten (10) calendar days after notification of the award of the Contract or failure to provide the payment and performance bonds and proof of insurance as required by the Contract Documents, the District shall have the right to award the Contract to another bidder and declare the bid security forfeited. The District reserves the right to pursue all other remedies in law or equity relating to such a breach including, but not limited to, seeking recovery of damages for breach of contract. Failure to provide bid security, or bid security in the proper amount, will result in rejection of the bid.

7. Withdrawal of Bid Proposals. Bid proposals may be withdrawn by the bidders prior to the time fixed for the opening of bids, but may not be withdrawn for a period of ninety (90) days after the opening of bids, except as permitted pursuant to Public Contract Code §5103.

8. Addenda or Bulletins. The District reserves the right to issue addenda or bulletins prior to the opening of the bids subject to the limitations of Public Contract Code §4104.5. Any addenda or bulletins issued prior to bid time shall be considered a part of the Contract Documents.

9. Bonds. The successful bidder shall be required to submit payment and/or performance bonds as specified in and using the bond forms included with the Contract Documents. All required bonds shall be based on the maximum total contract price as awarded, including additive alternates, if applicable.

10. Rejection of Bids and Award of Contract. The District reserves the right to waive any irregularities in the bid and reserves the right to reject any and all bids. The Contract will be awarded, if at all, within ninety (90) calendar days after the opening of bids to the lowest responsible and responsive bidder, subject to Governing Board approval. The time for awarding the Contract may be extended by the District with the consent of the lowest responsible, responsive bidder.

11. Execution of Contract. The successful bidder shall, within ten (10) calendar days of the Notice of Award of the Contract, sign and deliver to the District the executed Contract along with the bonds and certificates of insurance required by the Contract Documents. In the event the successful bidder fails or refuses to execute the Contract or fails to provide the bonds and certificates as required, the District may declare the bidder's bid deposit or bond forfeited as liquidated damages, and may award the work to the next lowest responsible, responsive bidder, or may reject all bids and, in its sole discretion, call for new bids. In all cases, the District reserves the right, without any liability, to cancel the award of

Contract at any time prior to the full execution of the Contract.

12. Drawings and Specifications. All drawings, specifications and other documents used or prepared during the project shall be the exclusive property of the District.

13. Evidence of Responsibility. Upon the request of the District, a bidder shall submit promptly to the District satisfactory evidence showing the bidder's financial resources, the bidder's experience in the type of work being required by the District, the bidder's availability to perform the Contract and any other required evidence of the bidder's qualifications to perform the Contract and any other required evidence of the bidder's qualifications and responsibility to perform the Contract. The District may consider such evidence before making its decision to award the Contract. Failure to submit requested evidence may result in rejection of the bid.

14. Taxes. Applicable taxes shall be included in the bid prices.

15. Bid Exceptions. Bid exceptions are not allowed. If the bidder has a comment regarding the bid documents or the scope of work, the bidder shall submit those comments to the District for evaluation at least five working days prior to the opening of the bids. No oral or telephonic modification of any bid submitted will be considered and a sealed written modification may be considered only if received prior to opening of bids. E-mailed or faxed bids or modifications will not be accepted.

16. Discounts. Any discounts which the bidder desires to provide the District must be stated clearly on the bid form itself so that the District can calculate the net cost of the bid proposal. Offers of discounts or additional services not delineated on the bid form will not be considered by the District in the determination of the lowest responsible responsive bidder.

17. Quantities. The quantities shown on the plans and specifications are approximate. The District reserves the right to increase or decrease quantities as desired.

18. Prices. Bidders must quote prices Freight on Board (F.O.B.) unless otherwise noted. Prices should be stated in the units specified and bidders should quote each item separately. If multiple line items of product, proposal shall be accompanied by a detail sheet, by unit cost, to the District accordingly. In the bid proposal form, vendor proposal shall write "see attached" for a total bid. This will allow the District to analyze all products submitted.

19. Samples. On request, samples of the products being bid shall be furnished to the District.

20. Special Brand Names/Substitutions. In describing any item, the use of a manufacturer or special brand does not restrict bidding to that manufacturer or special brand, but is intended only to indicate quality and type of item desired, except as provided in §3400 of the Public Contract Code. Substitute products will be considered either prior to or after the award of the Contract in accordance with §3400 and as set forth in either the Supplemental Conditions or the Specifications. All data substantiating the proposed

substitute as an "equal" item shall be submitted with the written request for substitution. The District reserves the right to make all final decisions on product and vendor selection.

21. Container Costs and Delivery. All costs for containers shall be borne by the bidder. All products shall conform to the provisions set forth in the federal, county, state and city laws for their production, handling, processing and labeling. Packages shall be so constructed in ensure safe transportation to point of delivery.

22. **Bid Negotiations. A bid response to any specific item of this bid using terms such as "negotiable," "will negotiate," or similar, will be considered non-responsive.**

23. Prevailing Law. In the event of any conflict or ambiguity between these instructions and state or federal law or regulations, the latter shall prevail. All equipment to be supplied or services to be performed under the bid proposal shall conform to all applicable requirements of local, state and federal law, including, but not limited to, Labor Code §§1771, 1778 and 1779.

24. Allowances. An "allowance" means an amount included in the bid proposal for work that may or may not be included in the Project, depending on conditions that will become known only after the Project is underway.

25. Subcontractors. Pursuant to the Subletting and Subcontracting Fair Practices Act, Public Contract Code §§4100-4114, every bidder shall, on the enclosed Subcontractor List Form, set forth:

    a. The name and location of the place of business of each Subcontractor who will perform work or labor or render service to the bidder in or about the work or fabricate and install work in an amount in excess of one-half (1/2) of one percent (1%) of the bidder's total bid.

    b. If the bidder fails to specify a Subcontractor for any portion of the work to be performed under the contract in excess of one-half (1/2) of one percent (1%) of the bidder's total bid, bidder agrees that bidder is fully qualified to and shall perform that portion of the work. The successful bidder shall not, without the written consent of the District or compliance with Public Contract Code §§ 4100 - 4114, either:

        1) Substitute any person as Subcontractor in place of the Subcontractor designated in the original bid;

        2) Permit any subcontract to be voluntarily assigned or transferred or allow the work to be performed by anyone other than the original Subcontractor listed in the bid; or

        3) Sublet or subcontract any portion of the work in excess of one-half (1/2) of

one percent (1%) of the total bid as to which the bidder's original bid did not designate a Subcontractor.

26. Examination of Contract Documents. Before submitting a bid proposal, all bidders shall carefully examine the Contract Documents, including and specifications, shall visit the site of the proposed work, and shall fully inform themselves of all conditions in and about the work site, as well as applicable federal, state and local laws and regulations that may affect the work. No bidder shall visit the site without prior authorization of the District. Bidders shall contact a local district representative to make site visits.

27. Form and Approval of Contract. The Contract Documents must be approved by the Governing Board of the District and its legal counsel. The bidder selected by the District shall execute the Contract provided by the District.

28. Licenses and Permits. Each bidder, and its Subcontractors, if any, shall at all times possess all appropriate and required licenses or other permits to perform the work as identified in the Contract Documents. Upon request, each bidder shall furnish the District with evidence demonstrating possession of the required licenses or permits.

29. Denial of Right to Bid. Contractors or Subcontractors who have violated state law governing public works shall be denied the right to bid on this public works contract pursuant to California Labor Code § 1777.7.

30. Bidders Interested in More Than One Bid. No person, firm, or corporation shall make, or file, or be interested in more than one bid. However, a person, firm, or corporation that has submitted a sub-proposal to a bidder, or that has quoted prices of materials to a bidder, is not thereby disqualified from submitting a sub-proposal or quoting prices to other bidders or from submitting a prime proposal.

31. Contractor's State License Board. Contractors and Subcontractors are required by law to be licensed and regulated by the California Contractors' Contractors' License Board.

32. Fingerprinting. **This Section applicable to K-12 only.**

33. Disabled Veterans Participation Goals. **This Section is applicable to K-12 only.**

34. Labor Compliance Program. This contract **is** ____/ **is not** **X** subject to a **labor** compliance

36. Bid Protest. Any bid protest must be in writing and received by the District Office before 5:00 p.m. no later than five (5) working days following bid opening and must comply with the following requirements:

a. The bid protest must contain a complete statement of the basis for the protest, and all supporting documentation.

b. The party filing the protest must have actually submitted a bid for the Project. A Subcontractor of a bidder submitting a bid for the Project may not submit a bid protest. A bidder may not rely on the bid protest submitted by another bidder, but must timely pursue its own protest.

c. The protest must refer to the specific portion or portions of the Contract Documents upon which the protest is based.

d. The protest must include the name, address and telephone number of the person representing the protesting bidder.

e. The bidder filing the protest must concurrently transmit a copy of the bid protest and all supporting documentation to all other bidders with a direct financial interest which may be affected by the outcome of the protest, including all other bidders who appear to have a reasonable prospect of receiving an award depending upon the outcome of the protest.

f. The bidder whose bid has been protested may submit a written response to the bid protest. Such response shall be submitted to the District before 5 p.m., no later than two (2) working days after the deadline for submission of the bid protest or other receipt of the bid protest, whichever is sooner, and shall include all supporting documentation. Such response shall also be transmitted concurrently to the protesting bidder and to all other bidders who appear to have a reasonable prospect of receiving an award depending upon the outcome of the protest.

g. The procedure and time limits set forth in this section are mandatory and are the bidder's sole and exclusive remedy in the event of bid protest. The bidder's failure to comply with these procedures shall constitute a waiver of any right to further pursue the bid protest, including filing a Government Code Claim or legal proceedings.

h. If the District determines that a protest is frivolous, the protesting bidder may be determined to be non-responsible and that bidder may be determined to be ineligible for future contract awards by the District.

i. A "working day" for purposes of this section means a weekday during which the District's office is open and conducting business, regardless of whether or not school is in session.

37. Piggybacking –

Other school districts and public agencies may purchase under this bid at the same prices, terms and conditions stated in these bid documents, at the discretion of the successful bidder.

Agencies participating in this bid shall be responsible for obtaining approval from their approving body of authority when necessary and shall hold the Marin Community College District harmless from any disputes, disagreements or actions which may arise as a result of using this bid.

The Marin Community College District waives its right to receive payment, and authorizes each district to make payment and place orders directly to the successful bidder.

Required Attachments:

1. Bid Proposal Form
2. Addenda
3. Subcontractor List Form
4. Worker's Compensation Certificate
5. Non-Collusion Affidavit
6. W-9 Request for Taxpayer Identification Number and Certification
7. Bidder's Questionnaire

To be completed by bidder and submitted with bid.

BID PROPOSAL FORM

Governing Board
Marin Community College District

Dear Members of the Governing Board:

The undersigned, doing business under the name of SECUREALL CORPORATION

_____, having carefully examined the location of the proposed work, the local conditions of the place where the work is to be done, the Notice Inviting Bids, the General Conditions, the Instructions to Bidders, the Plans and Specifications, and all other Contract Documents for the proposed **the District Wide Electronic Hardware/Software 17-0726**, ("Project"), and having accurately completed the Bidder's Questionnaire, proposes to perform all work and activities in accordance with the Contract Documents, including all of its component parts, and to furnish all required labor, materials, equipment, transportation and services required for the construction of the Project in strict conformity with the Contract Documents, including the Plans and Specifications as follows:

BASE BID:

For the sum of: SEE ATTACHED

_____**Dollars** (**$** _____

_____) **Alternate #1** _____

_____

Add/Subtract _____ **Dollars** (**$**_____)

ADDITIVE/DEDUCTIVE ALTERNATE *[if applicable]:*

Additive/Deductive Alternate #2 _____

Add/Subtract _____ Dollars ($_____)

Additive/Deductive Alternate #3 _____

Add/Subtract _____ Dollars ($_____)

The undersigned has checked carefully all the above figures and understands that the District is not responsible for any errors or omissions on the part of the undersigned in making this bid.

Contractor agrees to commence the work within the time specified in the Notice to Proceed. It is understood that this bid is based upon completing the work within the number of calendar days specified in the Contract Documents.

"Piggybacking" Documentation

Marin Community College District would also like to make the same pricing structures available to other area Board of Educations, UC's, CSU's and/or municipalities. Bidders shall indicate whether they shall extend pricing. Inclusion is not mandatory and will have no bearing on the contract award.

Agree to extend prices to other CC's, CSU's, UC's, School Districts,
or other public agencies within California RAS (Mark Acceptance by initialing line)

Do not agree to extend prices to other CC's, CSU's, UC's, School Districts,
or other public agencies within California _____(Mark denial by initialing line)

Other school districts, universities within the UC system of California, California State Universities (CSU's) and/or other public agencies may purchase under this bid at the same prices, terms and conditions stated in these bid documents, at the discretion of the successful bidder.

Agencies participating in this bid shall be responsible for obtaining approval from their approving body of authority when necessary and shall hold the Marin Community College District harmless from any disputes, disagreements or actions which may arise as a result of using this bid.

The Marin Community College District waives its right to receive payment, and authorizes each district to make payment and place orders directly to the successful bidder.

Vendor shall pay Marin Community College District a percentage of the sale, equal to .5% (1/2 of 1% of the total contract amount). Payment shall be made at the conclusion of the contract term by public agency or sixty (60) days from the final payment to the approved vendor by the public agency.

To be completed by bidder and submitted with bid.

ADDENDA:

Receipt of the following addenda is hereby acknowledged:

Addendum # 1 Dated: 8/1/17 Addendum # 4 Dated: 8/1/17
Addendum # 2 Dated: 8/1/17 Addendum # 5 Dated: 8/1/17
Addendum # 3 Dated: 8/1/17 Addendum # 6 Dated: 8/1/17

Respectfully Submitted,

Company: SECUREALL CORPORATION

Address: 695 WOBURN COURT
MOUNTAIN VIEW, CA. 94040

By: RICHARD SCHAFFZIN
(Please Print Or Type)

Signature: Richard Schaffzin

Title: CEO

Date: 7/31/17

Phone: 650-704-2725

Contractor's License No: N/A Expiration Date _____

To be completed by bidder and submitted with bid.

SUBCONTRACTOR LIST FORM

Each Bidder shall list below the name and location of place of business for each Subcontractor who will perform a portion of the Contract work in an amount in excess of 1/2 of 1 percent of the total contract price. The nature of the work to be subcontracted shall be described.

DESCRIPTION OF WORK	SUBCONTRACTOR NAME	LOCATION OF BUSINESS

To be completed by bidder and submitted with bid.

WORKERS' COMPENSATION CERTIFICATE

Labor Code §3700 in relevant part provides:

> "Every employer except the State shall secure the payment of compensation in one or more of the following ways:
>
> (a) By being insured against liability to pay compensation in one or more insurers duly authorized to write compensation insurance in this State.
>
> (b) Be securing from the Director of Industrial Relations a certificate of consent to self-insure, which may be given upon furnishing proof satisfactory to the Director of Industrial Relations of ability to self-insure and to pay any compensation that may become due to his employees."

I am aware of the provisions of §3700 of the Labor Code which require every employer to be insured against liability for workers' compensation or to undertake self-insurance in accordance with the provisions of that Code, and I will comply with such provisions before commencing the performance of the work of this Contract and will require all Subcontractors to do the same.

SECURE ALL CORPORATION
Contractor

By: _____

In accordance with Article 5 (commencing at §1860), Chapter 1, Part 7, Division 2 of the Labor Code, the above certificate must be signed and filed with the awarding body prior to performing any work under this Contract.

To be completed by bidder and submitted with bid.

.NONCOLLUSION AFFIDAVIT

State of California

County of (SANTA CLARA)

RICHARD SCHAFFZIN, being first duly sworn, deposes and says that he or she is CEO of SECUREALL CORP. the party making the foregoing bid, and affirms that the bid is not made in the interest of, or on behalf of, any undisclosed person, partnership, company, association, organization, or corporation; that the bid is genuine and not collusive or sham; that the bidder has not directly or indirectly induced or solicited any other bidder to put in a false or sham bid, and has not directly or indirectly colluded, conspired, connived, or agreed with any bidder or anyone else to put in a sham bid, or that anyone shall refrain from bidding; that the bidder has not in any manner, directly or indirectly, sought by agreement, communication, or conference with anyone to fix the bid price of the bidder or any other bidder, or to fix any overhead, profit, or cost element of the bid price, or of that of any other bidder, or to secure any advantage against the public body awarding the contract of anyone interested in the proposed contract; that all statements contained in the bid are true and correct; and, further, that the bidder has not, directly or indirectly, submitted his or her bid price or any breakdown thereof, or the contents thereof, or divulged information or data relative thereto, or paid, and will not pay, any fee to any corporation, partnership, company association, organization, bid depository, or to any member or agent thereof to effectuate a collusive or sham bid.

I certify (or declare) under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Date: 8/1/17 _____
Signature

State of CALIFORNIA, County of SANTA CLARA

On_____before me,_____, personally appeared

_____

personally known to me or proved to me on the basis of satisfactory evidence to be the person(s) whose name(s) is/are subscribed to the within instrument and acknowledged to me that he/she/they executed the same in his/her/their authorized capacity (ies), and that by his/her/their signature(s) on the instrument the person(s), or the entity upon behalf of which the person(s) acted, executed the instrument.

WITNESS my hand and official seal.

_____
Signature of Notary Public

A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

State of California, County of Santa Clara)ss. On 8/1/17 before me, Sunita Singh, Notary Public, personally appeared Richard Schaffzin, who proved to me on the basis of satisfactory evidence to be the person(s) whose name(s) is/are subscribed to the within instrument and acknowledged to me that he/she/they executed the same in his/her/their authorized capacity(ies), and that by his/her/their signature(s) on the instrument the person(s), or the entity upon behalf of which the person(s) acted, executed the instrument. I certify under PENALTY OF PERJURY under the laws of the State of California that the foregoing paragraph is true and correct. WITNESS my hand and official seal.

SUNITA SINGH
Notary Public - California
Santa Clara County
Commission # 2171583
My Comm. Expires Nov 18, 2020

To be completed by bidder and submitted with bid.

BIDDER'S QUESTIONNAIRE

District Wide Electronic Hardware/Software Installation Phase 2

TO THE BIDDER: **#15-0908**

In making its award the Governing Board will take into consideration Bidder's experience, financial responsibility and capability. The following questionnaire is a part of the bid. Any bid received without this completed questionnaire may be rejected as nonresponsive. The District will use, but will not be limited to, the information provided herein for evaluating the qualifications and responsibility of the bidder and the bidder's organization to carry out satisfactorily the terms of the Contract Document. The questionnaire must be filled out accurately and completely and submitted with the bid. Any errors, omissions or misrepresentation of information may be considered as a basis for the rejection of the bid and may be grounds for the termination of any subsequent contract executed as a result of the bid.

A. Description of Bidder's Organization

1. Firm Name SECUREALL CORPORATION
2. Address 695 WOBURN COURT, MOUNTAIN VIEW, CA. 94040
3. Telephone Number 650-704-2725
4. Type of Organization
   a. Corporation? Yes ✓ No ____

If yes, list officers and positions, and the State in which incorporated.
RICHARD SCHAFFZIN, CEO, CFO, SEC., CA. C CORP.

If the Bidder corporation is a subsidiary, give name and address of parent corporation:

b. Partnership? Yes____ No ✓
If yes, list partner's names and addresses
General Partners:

Limited Partners:

c. Individual Proprietorship? Yes ____ No ✓

If yes, list name and address of proprietor:

B. Nature of Operations

1. How long have you been engaged in the contracting business under your present business name? 13 YEARS

2. How many years of experience does your business have in work similar to that called for under this bid? 9 YEARS

3. Have you now contracts, or have you ever contracted, to provide construction for any school district, community college district or county office of education in the State of California? Yes ✓ No ____

   a. If "yes," on a separate attached sheet, provide the following information for all construction projects you have had with school districts, community college districts, or county offices of education during the last four (4) years:

      1. Year contract awarded
      2. Type of work
      3. Contract completion time called for/actual completion time
      4. Contract price
      5. For whom performed, including person to call for reference and telephone number
      6. Location of work
      7. Number of stop notices filed
      8. For each contract, list any lawsuits filed relating to that contract in which you were a defendant or plaintiff
      9. Amount of liquidated damages assessed

   b. On a separate attached sheet, provide the following information for all construction contracts of a similar nature as called for in this bid that you have had with entities other than school districts, community college districts and county offices of education during the last four (4) years:

      1. Year contract awarded
      2. Type of work
      3. Contract completion time called for/actual completion time
      4. Contract price
      5. For whom performed, including person to call for reference and telephone number
      6. Location of work
      7. Number of stop notices filed
      8. For each contract list any lawsuits filed relating to that contract in which you were a defendant or plaintiff
      9. Amount of liquidated damages assessed

   c. For each construction contract that you have failed to complete within the contract time in the last four (4) years, please state the reasons for the untimely performance. NONE.

C. Financial and Credit Data

1. If your bid is considered for award, and if requested by the District, will you supply the following data? Yes ✓ No _____

   a. Names and addresses of any banks where you regularly do business.

   b. The names and addresses of any banks, finance companies, dealers, suppliers, or others where you have notes or loans.

   c. Give credit references, including at least three trade or industry suppliers with whom you regularly deal.

2. Will you submit on request a balance sheet for the past three (3) years?
   Yes ✓ No _____

3. Where have you engaged in the construction business or any other type of business in the last five (5) years?

Name of Business	Location	Type of Business	Years in Business

If any of the business endeavors referred to above are no longer operating, or you are no longer associated with them, please give brief details:

_____
_____
_____

4. The following surety companies may be contacted as references as to the financial responsibility and general reliability of the bidder:

Surety Name	Contact Person	Phone Number
N/A		

I certify under penalty of perjury that the foregoing is true and correct. Executed at MOUNTAIN VIEW, California, on 8/1, 20 17.

Signature of Bidder _____

Name *(print)* RICHARD SCHAFFZIN

Guarantee & Warranty

Vendor hereby guarantees and warrants its work on the Project for a period of three (3) years from the date of the filing of Notice of Completion as follows.

Vendor shall promptly repair or replace to the satisfaction of the District any or all work that appears defective in workmanship, equipment and/or materials for whatever reason, ordinary wear and tear and unusual abuse or neglect excepted, together with any other work which may be damaged or displaced in so doing.

Vendor agrees to promptly correct and remedy any failure by the Vendor to conform its work, activities and services to the requirements of the Contract Documents.

In the event of the Vendor's failure to comply with the above-mentioned obligations within ten (10) calendar days of notice, or sooner if required by an emergency, Contractor hereby authorizes the District to have the defects or deficiencies repaired, remedied, corrected and made good at Contractor's expense, and Contractor shall pay the costs and charges therefore upon demand. The Surety agrees to be responsible for these costs and charges as well.

SAMPLE

EXAMPLE OF NOTICE OF AWARD

To:

Project Description: District Hardware and Software

The District has considered the bid submitted by you for the above described work in response to its Notice Inviting Bids, dated_____.

You are hereby notified that your bid has been accepted for items in the amount of:

_____
_____ ($
_____).

You are required by the Information for Bidders to execute the Agreement and furnish the Performance Bond and Payment Bond (if Contract Price is $25,000 or more), and certificates of insurance within ten (10) days from the date of receipt of this Notice.

If you fail to execute the Agreement and to furnish the bonds within ten (10) days from the date of receipt of this Notice, District will be entitled to consider all your rights arising out of its acceptance of your bid as abandoned and as a forfeiture of your Bid Bond. The District will be entitled to such other rights as may be granted by law.

You are required to return an acknowledged copy of this Notice of Award to the District.

Dated this_____day of_____, 201__.

By _____
Authorized District Signature

Receipt of this above Notice of Award is hereby acknowledged by:

_____, this is the _____

day of_____, 201_.

By _____

Title _____

SAMPLE

EXAMPLE OF NOTICE TO PROCEED

SAMPLE

To: Date:

PROJECT:

You are hereby notified to commence work in accordance with the Agreement dated,

_____, 20 , on or before_____, 20__, and you

are to complete the work_____consecutive calendar days thereafter.

By: _____

Authorized District Signature

Part 1 – General

1.1 DESCRIPTION

Provide, install, program, configure and activate equipment that shall provide a complete and functional, centrally controlled Access Control and Alarm Monitoring System (ACAMS) with local and remote monitoring capabilities. The system shall be completely "turn-key" and shall include all the components listed in Section 2a of this specification.

1. Work Included - The specified system shall be comprised of four primary components described below:

    a. Central Server shall be rack mountable and housed in a telecommunication closet with connection to a facility's LAN. The server shall be managed with a user-friendly GUI based software platform for system control and shall be capable of running a single building or an entire campus. The server shall be equipped with sufficiently sized core processors and memory to control and manage a campus or campuses and be able to handle up to 10,000 doors. The server software shall include:

        i. Dynamic user fields to program system parameters, personal user information and other programmable features. All access privileges are defined at the server but then downloaded to the doors where access enforcement takes place.

        ii. Alarms that identify a system problem (i.e. low battery) or alarm states (i.e. door ajar or forced entry) and any required corrective action by the system administrator. Alarms shall be visible at the server screen or can be sent via email or text to authorized personnel.

        iii. System Partitioning: optional function that provides the ability to partition the system to enable local administrators to create programming changes within their authorized zones. Partitioning rights and zones shall be set up and controlled by the Master Administrator.

        iv. Availability of zones (collections of door locks, buildings, etc) and user access groups (collection of scheduled access to rooms) minimize the labor necessary to define allowed access throughout a

campus. An access group can have up to 500 door schedules and a user can be a member of up to 100 access groups.

v. The server shall provide constant monitoring of the health of the entire access control system.

vi. Multi-layer encryption provides system security to help ensure the system cannot be hacked or compromised by outside influences with malicious intent.

1. System must use at least AES128 (or equivalent) symmetric encryption on all communication links.
2. All devices and server shall be authenticated by PKI (Public Key Infrastructure).
3. Each device (lock or key) shall have a separate encryption certificate.
4. System administrator shall have the capability to periodically change encryption certificates.

vii. Server may be programmed locally (using SSL) or remotely via VPN tunnel.

viii. Easy interface with the most common Enterprise Resource Planning (ERP) applications.

ix. Access history shall be maintained for up to one year and must be easily accessible.

b. Wireless router (access point) provides all communication between the Central Server and the wireless access control units. Each router shall:

i. Be connected to the Central Server using CAT5E or higher network cabling.

ii. Have the ability to be powered via Power-over-Ethernet (POE) or using an external 5V DC power supply.

iii. Contain internal back-up batteries capable of providing up to 6 hours of continuous operation time.

iv. Utilize Extreme Low Power RF communication technology operating at 2.4HGz in the ISM band that does not interfere with, or receive interference from, other existing wireless platforms.

v. Have a communication range of up to1800 feet in open space and the ability to control up to 1000 lock units within the communication range. Internal walls and other obstructions could reduce the range and the number of lock units controlled by each router. Careful planning and site surveys shall be required to determine the best locations for wireless routers.

1. For redundancy, best practice shall be to design the system to allow each lock to communicate with at least two routers.

vi. Multi-layer encryption provides system security to help ensure the system cannot be hacked or compromised by outside influences with malicious intent.

1. System must use at least AES128 (or equivalent) symmetric encryption on all communication links.

2. All devices and server shall be authenticated by PKI (Public Key Infrastructure).

3. Each device (lock or key) shall have a separate encryption certificate.

4. System administrator shall have the capability to periodically change encryption certificates.

c. Wireless access control unit with or without locking hardware. Units designed with locking hardware shall be available in either mortise or cylindrical style lock sets. The access control units must also be compatible with Von Duprin Series 98/99 exit devices. Both shall be equipped with access control electronics and door open/ajar sensor integrated into the unit. These lock units shall be mounted directly in the door within range of at least one Wireless Router. Wireless access control units without lock hardware (powered wall readers) shall be used in conjunction with powered main doors, motorized garage or gate openers. These devises shall operate as definable range sensors with direct connection to the powered openers. For individual device mounting details, please see associated drawings. Wireless access control units shall:

i. Utilize patented Extreme Low Power RF communication technology that does not interfere with or receive interference from other existing wireless platforms.

ii. Run on three AA standard alkaline batteries for mortise or cylindrical lock sets, typical battery life with normal usage up to 4 years. Exit

devices shall be equipped with 6 C-cell batteries and have this same lifetime. Powered wall readers shall run on voltage (12V/24V) supplied from the electronic door activation equipment. Backup batteries are also standard in each powered wall reader.

iii. Use approved Access Control List (ACL). Software for each unit shall be downloaded from the central server and locally stored. All access control decisions shall be made at the unit giving the system the ability to continue operating as normal in the event of a power failure.

iv. Be capable of supporting up to 1000 users, with upgradable memory for up to 70,000 users.

v. Use Multi-layer encryption which provides system security to help ensure the system cannot be hacked or compromised by outside influences with malicious intent. Each lock shall have its own encryption key, which can be modified as desired via secure over- the-air administrative command.

1. System must use at least AES128 (or equivalent) symmetric encryption on all communication links.
2. All devices and server shall be authenticated by PKI (Public Key Infrastructure).
3. Each device (lock or key) shall have a separate encryption certificate.
4. System administrator shall have the capability to periodically change encryption certificates.

vi. Employ tamper protection and alarm issuance when the door lock is struck by a heavy object or tampered with in any way.

vii. Obtain secure over-the-air firmware upgrades. Code changes shall be complete in less than one minute.

viii. Store up to 30 calendars to create different work schedules for all user groups.

ix. Have access control by time and date; may be programmed as on- going access or single events, all decision making resident in the lock.

x. Have access data logging and door ajar sensing via sensors integrated into the lock unit. Rules for door ajar alarm shall be user definable.

xi. Be capable of controlling multiple types of portals, i.e. office doors, main doors, gates, garages, etc.

xii. Have programmable activation distances which can be different for each lock unit types (i.e. office doors can have activation distance of a few inches to several feet while garage access can be up to sixty feet.)

xiii. Be either :

1) Fully self-contained for installation within inside doors or;

2) Independent controllers that interface with main door or garage automatic opening systems, including panic hardware and handicap requirements. The latter unit shall interoperate with ADA push-button requirements.

xiv. Be capable of enabling real-time lockdown (<1 minute for 3,000 doors) for an entire campus or any subset of a campus without the need for partitioning.

1. During lockdown, first responders shall not be prevented from entering a building as long as they have a valid key. For response to an afterhours or emergency event, a Knox box shall be installed outside the main entrance where a "master" key shall be located. A minimum of one router shall be placed within an acceptable communication range of the Knox box to allow periodic updates to the "master" key located within.

2. There shall be at least 4 user-defined threat levels to determine if an individual is allowed access during lockdown.

3. A user's access group shall define the maximum threat level at which access is allowed.

xv. Constantly monitor battery usage and;

1. generate a "low battery voltage caution alarm" when voltage drops below a user defined threshold.

2. generate an "imminent failure warning alarm" when voltage drops below a critical threshold in which a lock is not guaranteed to operate.

xvi. Allow egress from inside a room/building without a "request to exit" device.

xvii. Enable an "office mode" setting such that;

1. A door shall be automatically unlocked per a specified schedule, including days of the week, start and end times, start and end dates, and holiday calendar.

2. An enhanced office mode shall be available whereby a door goes into the unlocked state only after the first valid user checks in. The standard office mode schedule is then followed.

3. The unlocked condition shall have the ability to be manually overridden at the door by the door "owner." The state of the door can be changed manually an unlimited number of times during the day.

xviii. Be equipped with an "auxiliary power supply" that will enable a door to be opened with a valid key, even when the internal batteries are below critical level.

xix. Have the ability to add "tailgate detection" equipment to ensure that only authorized individuals enter a building.

d. Hands-free transceiver carried by all users that require access to any lock on campus. Hands-free transceiver shall:

i. Utilize patented Extreme Low Power RF communication technology that does not interfere with or receive interference from other existing wireless platforms.

ii. Run on standard off-the-shelf coin cell battery and have typical battery life with normal usage of up to 4 years.

iii. Use Multi-layer encryption which provides system security to help ensure the system cannot be hacked or compromised by outside influences with malicious intent.

1. System must use at least AES128 (or equivalent) symmetric encryption on all communication links.

2. All devices and server shall be authenticated by PKI (Public Key Infrastructure).

3. Each device (lock or key) shall have a separate encryption certificate.

4. System administrator shall have the capability to periodically change encryption certificates.

iv. Have multi-distance capability allowing a single key to be capable of activating an unlimited number of different types of doors, each at a different range. The range is programmed into the door lock via the server.

v. In addition to multi-distance capability, control shall be available within a transceiver so each user can have custom tailored lock activation distance depending on their physical need (i.e. wheelchair vs. normal user). The transceiver shall also operate automatic door openers when activation distance is reached.

vi. Have the ability to remove lost transceivers from the system by either the system administrator and/or the user. The user shall have the ability to deactivate and report a lost or stolen key via the internet through a secure web portal. Reactivation may only be performed by the system administrator.

vii. Shall receive firmware upgrades performed periodically through secure over- the-air communication with the router.

viii. Have the ability to access stored user information including a picture of a key holder at a monitoring station to ensure the individual being granted access is the key owner.

1.2 BASIC DEFINITIONS

1. Abbreviations:

a. ACAMS Access Control and Alarm Monitoring System

b. IDF Intermediate Distribution Frame

c. IP Internet Protocol

d. MDF Main Distribution Frame

e. Server Central Server Room

f. Regional Server in MDF Room

g. SCR Security Control Room

h. SSL Secure Sockets Layer

i. VPN Virtual Private Network

j. PoE Power over Ethernet

1.3 PERFORMANCE

Furnish and install a complete ACAMS which meets or exceeds the following performance requirements.

1. NEC Class II standards:

    a. Furnish and install the ACAMS in such a way that it is fully compliant with the Class II limited power requirements of the NEC.

2. Underwriters' Laboratories Compliance:

    a. Locking units mounted directly on doors must meet all UL standards for Fire Tests of Door Assemblies. The balance of ACAMS will fully satisfy all UL 294 requirements, both in terms of its design and documentation, and also in the completed installation.

3. Ethernet Connectivity:

    a. Furnish and install ACAMS hardware and software possessing the ability to connect routers, servers and workstations over an existing LAN or WAN.

4. Report Management

    a. The system shall have integrated reports that can be used to analyze user activity, including event and access logs.

5. Alarm Presentation

    a. Alarm management screen must have the following attributes and functions:

i. ACAMS software must present alarms on the alarm screen in a "double-sort" fashion, with priority as the first sort, and initiation time as the second sort. Sort order must refresh in real time upon each addition or deletion of active alarm events.

ii. Must have the ability to govern permissions granted to alarm management screen operators, and the option to deny them the ability to modify sort preferences.

6. Administrator Permissions

a. Furnish and install ACAMS which offers a "matrix" approach to the granting of administrator permissions. Provide different groups of administrators with the ability to manipulate any programmable set of system functions to which they are granted permission.

b. Provide the capability of limiting or controlling administrators' ability to view, edit, add or delete any fields or attributes of the database.

7. Operator Audit Trail

a. Create a record of, and provide the ability to create reports of, all operator actions within the ACAMS software, including:

i. The time a change was made by an operator.

ii. The operator's name.

iii. The item's state before the change was made.

iv. The item's state after the change.

1.4 SYSTEM TRAINING

1. System integrator shall furnish personnel to execute the training plan.
2. Establish a specific schedule that meets the convenience of customer.
3. Provide training literature and outlines at the beginning of each session.
4. Operator and management training:

a. Provide a minimum of 36 hours total operator and management training time, with a mixture of class time and on-call time per customer/District.

b. Include system operation and database management.

5. Technical maintenance training:

a. Provide a minimum of 16 hours total technical maintenance training time per customer/District.

1.5 DATABASE ASSISTANCE

1. System integrator shall coordinate with the administrator to set up the initial database requirements and formats. Provide appropriate forms and written instructions. Provide examples of the sequence of completion for all related forms.

1.6 SUBMITTALS

1. Provide submittals as required.

2. At time of bid, provide a letter stating that the security integrator is a factory certified installation contractor.

3. Submit proposed shop test schedule and procedure.

4. Submit training plan and schedule.

5. Submit as-built documentation.

6. Submit spare parts list, if any. See Section 3.07.

PART 2 – PRODUCTS

2.0.1 WORK INCLUDED

1. Furnish a complete and operable system as described in these specifications and in the associated drawings. It shall be the responsibility of the integrator/contractor to provide a complete and operable system.

2. Review the Drawings and Schedules to identify any additional components required to provide a complete and operable system. Verify all quantities with those shown on the design Drawings and Details.

3. The ACAMS central components shall all be from the same system manufacturer. All locks, systems and installation must meet Title II & III of the Americans with Disabilities Act of 1990, updated 2012.

4. All locks, systems and installation must meet all applicable sections of National Fire Protection Association (NFPA) codes and regulations

2.1 MATERIALS

1. Furnish and install a complete system which includes the following equipment:
    a. Central Server
    b. Software
    c. PoE switches (provided by customer)
    d. Wireless Router (Access Points)
    e. Wireless Access Control Units (lock units or sensors)
    f. Transceivers
    g. Network cabling to wireless routers and power wall readers (can be supplied by customer or system integrator)
    h. Von Duprin 98/99 series panic hardware where needed
2. The following items shall be provided as a part of the ACAMS.
    a. VPN equipment for remote oversight and programming, if required
        a. total of (3) three automatic key readers for ease of data entry at key issue and key return station.
        c. total of (3) auxiliary power supply that enables entry even when batteries are exhausted.
        d. total of (8) eight In-car units for gate access for campus police and service vehicles.
        e. total of (100) one-hundred additional u-keys.

f. install single occupancy restroom lock sets that allow for locking the door from the inside. Contractor is responsible for insuring the count of restrooms and locksets.

g. furnish a total of (20) key pad style locksets for various doors throughout the campuses where required by the District.

3. Customer or system integrator shall be responsible for the installation, termination, testing and labeling of all network cabling connecting the Wireless Routers to the Central Server. Network cabling shall include all patch cords from patch panel to switch and switch to server.

4. Furnish and install all materials identified in the Drawings. Integrator shall perform a detailed site survey to confirm item unit counts and quantities with customer and/or System Designer.

5. Carefully review all details for exact type and quantity of parts and devices required to support field and head end security apparatus.

6. Furnish and install materials, equipment, software, and any other apparatus or support necessary to comply with the requirements articulated above in Part 1.01, DESCRIPTION.

7. Winning bidder shall be responsible for replacing any out of code "panic hardware" with Von Duprin 98/99 series hardware and integrating said hardware with new electronic lock system.

3.1 SYSTEM INSTALLATION

1. Confirm that the locking hardware for individual doors is consistent with the security design.

2. System Workstations Install:

a. Loaded Client workstation software on the server located in the MDF rack.

b. Remote workstation, for remote access by the security manager.

Software and configuration only, PC to be customer provided.

3. Central Server and associated equipment. Install in the MDF room, refer to plans and details.

4. Install all door controllers per plans and details.

5. Winning bidder shall be responsible for replacing any out of code "panic hardware" with Von Duprin 98/99 series hardware and integrating said hardware with new electronic lock system.

3.2 SYSTEM PROGRAMMING

1. Program the system database. Program the system "from the ground up" using consistent programming and naming conventions.

2. Program the hardware as defined in the Detail Package and on the Drawings.

3. Coordinate with the customer in the use of setting up the permissions for the system and definition of naming convention and abbreviations.

4. Point descriptions:

a. Input a description for each point.

b. Use descriptions that are consistent in form and character.

c. Use all uppercase characters.

d. Use consistent abbreviations throughout the database. If a word is abbreviated in one location, always use the same abbreviation.

i. Submit any additions or changes to customer for approval before loading the point descriptions in the database.

e. Geographic directions:

i. Use N for North, S for South, E for East, and W for West.

ii. Use only NE, NW, SE, or SW for combined directions.

iii. Use a single character (or combined characters) between two spaces preceding the name to qualify a building area, room, door, or device.

f. Order of Information:

i. Fixed and consistent sequence: building (1 character), space, floor (2 characters), space, room or area, space, description of device or object

ii. Examples.

1. 7 01 LBY DR
2. 7 01 LBY FIRE PNL ALM
3. 9 04 BLDG OFFICE

3.3 SYSTEM TESTING

1. Site Test: After the system is installed:
   a. Perform the appropriate system tests.
   b. In addition, perform all manufacturer-recommended tests.

3.4 FINAL ACCEPTANCE TESTING

1. Integrator to perform field inspection and testing.
2. Integrator to provide the following As-Built documents:
   a. Drawings to define the system configuration and settings.
   b. Testing sheets to be filled out per point.
   c. IP addresses provided for all devices, as required.
   d. Cut sheets provided for each device.

3.5 WARRANTY SERVICE

1. Provide limited manufacturers' warranty that shall warrant the goods against faulty workmanship or the use of defective materials, and that such goods will conform to Seller's written specifications, drawings, and other descriptions for a period of three (3) years.

2. Service organization:

a. Factory-trained by system manufacturer.
Location within 100 miles of the job site.

3. Fully qualified repair and maintenance personnel within the service organization:

a. Available on a next day basis, 365 days a year.

b. Generally able to respond within a maximum 4-hour response time during normal business hours.

4. Normal Service for Equipment:

a. Defined as minor repairs, adjustments, or any service required for the system to be fully functional, and which, at the customer's discretion, does not fall into the category of Emergency Service.

b. Provide at no additional cost to customer during normal business hours, between 7:00a.m. and 5:00 p.m., Monday through Friday.

c. Respond on a same-day basis for service calls requested by phone before 1:00 p.m. on a weekday.

d. If warranty service is requested after 1:00 p.m. on a weekday, or at any time on a weekend, respond on the next working day before 1:00 p.m.

5. Emergency service for Equipment:

a. Emergency service is defined as repairs, adjustments, parts, replacement of parts, or any service required to make the system fully functional and is beyond the category of Normal Service, at the option of the customer.

b. Provide at additional cost to customer according to labor rate schedule contractually agreed upon.

c. Respond within a 4-hour period, 24-hours per day, 365 days per year.

d. Upon award of contract, provide customer with a cost estimate for emergency service.

6. Maintenance Service for Software:

a. Provide at no additional cost to customer.

b. Respond within the next business day, during normal business hours.

7. Provide full factory technical support and same day shipping of replacement parts for all equipment.

3.6 SPARE PARTS

1. Prepare a list of all items that have a history of requiring repair or replacements of 12 months or less, are critical to the operation of the system, or are known to be long lead items for replacement.

2. Provide an inventory of spare parts for the items listed, as agreed with customer. These parts shall be stored on site at a facility of District's choosing, depending upon the criticality of the part and general availability.

   a. 100 electronic keys

   b. 10 door units of each type of lockset type

   c. 5 wireless routers

Addendum #1 8/1/17

Bidder's Questionnaire

Sections B 3a & B 3b

Addendum #1 8/1/17

Bidder's Questionnaire, Section B 3a

College of Marin

1. 2013, 2014, 2015, 2016
2. Deliver wireless, total security system
3. 2014, 2015, 2016, 2017 on-time
4. $79,353; $516,918; $315,875; $285,194
5. Greg Nelson, VP Finance & College Operations, 415-884-3101
6. Kentfield and Indian Valley campuses
7. None
8. None
9. None

Bidder's Questionnaire, Section B 3b

Santa Clara University

1. 2013, 2014, 2015, 2016
2. Deliver wireless, total security system
3. 2013, 2014, 2015, 2016 on-time
4. $203,765; $25,962; $38,831; $37,018
5. Chris Shay, VP Finance & Administration, 408-554-4300
6. Santa Clara and San Jose campuses
7. None
8. None
9. None

The Peninsula Regent, Retirement Community

1. 2013, 2014, 2015, 2016
2. Deliver wireless, total security system
3. 2013, 2014, 2015, 2016 on-time
4. $315,257; $51,885; $11,704; $27,669
5. Marianne Nannestad, Executive Director, 650-425-4214

Addendum #2 8/1/17

Guarantee & Warranty

Addendum #2 8/1/17

Guarantee & Warranty

Seller, except as otherwise hereinafter provided, warrants the goods against faulty workmanship or the use of defective materials, and that such goods will conform to Seller's written specifications, drawings, and other descriptions for a period of two (2) years. Seller warrants that at the time of delivery, Seller has title to the goods free and clear of any and all liens and encumbrances. These warranties are the only warranties made by Seller and can be amended only by a written instrument signed by an officer of Seller. All warranties that Seller provides to Buyer are solely for Buyer's benefit. Buyer may not transfer or assign any of these warranties. Continued use or possession of goods after expiration of the applicable warranty period stated above shall be conclusive evidence that the warranty is fulfilled to the full satisfaction of Buyer.

Seller's warranties as hereinabove set forth shall not be enlarged, diminished or affected by, and no obligation or liability shall arise or grow out of Seller's rendering of technical advice or service in connection with Buyer's order of the goods furnished hereunder. If the goods furnished by Seller fail to conform to Seller's exclusive limited warranty, Seller's sole and exclusive liability shall be (at Seller's option) to repair, replace or credit Buyer's account for any such goods which are returned by Buyer during the applicable warranty period set forth above, provided that (i) Seller is promptly notified in writing upon discovery by Buyer that such goods failed to conform to this contract with a detailed explanation of any alleged deficiencies, (ii) such goods are returned to Seller, F.O.B. Seller's plant, and (iii) Seller's examination of such goods shall disclose to Seller's satisfaction that such alleged deficiencies actually exist and were not caused by accident, misuse, neglect, alteration, improper installation, unauthorized repair or improper testing. If such goods are non-conforming, Seller shall reimburse Buyer for the transportation charges paid by Buyer for such

Addendum #3 8/1/17

Product Description

Addendum #3 8/1/17

Product Description

Part 1 - General

1.1 DESCRIPTION

SecureALL will, in conjunction with customer input, identify the necessary components to provide a complete, turn-key security system. SecureALL will deliver all components to customer, who will take responsibility for installing the equipment. SecureALL will provide, free of charge, installation training for customer employees if desired, or will work with customer to identify a capable third party to do the installation. SecureALL will provide periodic oversight to ensure installers are performing the task per specification.

Once installation is complete, SecureALL is available to train customer staff to program, configure and activate the turn-key security system. If customer does not have staff that can be trained to perform this function, SecureALL can put a Service Agreement in place to take on that responsibility. Please see attached price list for optional training and service.

Addendum #4 8/1/17

Price Lists

Year 1: September 2017-August 2018

Year 2: September 2018-August 2019

Year 3: September 2019-August 2020

SecureALL Price List*

* Volume price discounts apply to total unit quantity ordered within a category, i.e. locking hardware

**Escalation cost is built in at a not to exceed 5% per year. This is formatted to show a not to exceed price. Price may be less depending on the CPI, check with vendor for annual escalation

*** Standard terms are net 30. Discounts are available: 2% net 10; 1% net 20

		Year 1 of Contract September 2017- August 2018					
Locking Hardware		< 100	100 - 250	251 - 500	501 - 1000	1001 - 5000	> 5001
SA-CDR	Cylindrical Door Reader	742.50	675.00	641.25	607.50	573.75	540.00
SA-CRR	Cylindrical Restroom (Privacy) Reader	782.50	715.00	681.25	647.50	613.75	580.00
SA-MDR	Mortise Door Reader	819.50	745.00	707.75	670.50	633.25	596.00
SA-MRR	Mortise Restroom (Privacy) Reader	859.50	785.00	747.75	710.50	673.25	636.00
SA-ODR	Onity Door Reader Retrofit Kit	604.00	549.00	521.50	494.00	466.50	439.25
SA-OGD	Dual Outside Gate (Garage) Reader - Long Range	1402.50	1275.00	1211.25	1147.50	1083.75	1020.00
SA-OGR	Outside Gate (Garage) Reader - Long Range	852.50	775.00	736.25	697.50	658.75	620.00
SA-OPR	Onity Panic Hardware Reader Retrofit Kit	714.00	649.00	616.50	584.00	551.50	519.25
SA-PCD	Passage Cylindrical Door Reader	544.50	495.00	470.25	445.50	420.75	396.00
SA-PMD	Passage Mortise Door Reader	621.50	565.00	536.75	508.50	480.25	452.00
SA-PHM	Panic Hardware Mortise Device	N/A	N/A	N/A	N/A	N/A	N/A
SA-PHR	Panic Hardware Rim Device (Von Duprin 98/99) Retrofit Kit	1025.75	932.50	850.00	808.75	767.50	726.25
SA-PSR	Point of Sale Reader	797.50	725.00	688.75	652.50	616.25	580.00
SA-PWD	Dual Panic Wall Reader	1347.50	1225.00	1163.75	1102.50	1041.25	980.00
SA-PWR	Panic Wall Reader	797.50	725.00	688.75	652.50	616.25	580.00

Option Adders		< 100	100 - 250	251 - 500	501 - 1000	1001 - 5000	> 5001
C	SFIC Keyway Included	110.00	100.00	95.00	90.00	85.00	80.00
D	Dual Proximity and Smartcard Reader	165.00	150.00	142.50	135.00	127.50	120.00
G	Standard Falcon Cylindrical Keyway for PHR	110.00	100.00	95.00	90.00	85.00	80.00
H	Handle to Accommodate SFIC (core customer supplied)	27.50	25.00	23.75	22.50	21.25	20.00
K	10 Key Pushbutton	95.00	90.00	87.50	85.00	82.50	77.50
O	Outdoor Weatherization	110.00	100.00	95.00	90.00	85.00	80.00
P	Proximity Card Reader	110.00	100.00	95.00	90.00	85.00	80.00
S	Smartcard Reader	110.00	100.00	95.00	90.00	85.00	80.00

Ancillary Equipment		< 100	100 - 250	251 - 500	501 - 1000	1001 - 5000	> 5001
SA-APS	Auxiliary Power Supply	495.00					
SA-ITK	Installation Tool Kit	395.00					
SA-LST	Deadlatch Sensor Tester	295.00					
SA-SAT	Site Audit Tool Kit	995.00					
SA-UKR	Universal Key Reader	395.00					
SA-LOC	Locator	594.00	540.00	513.00	486.00	459.00	432.00
SA-ROU	Router	709.50	645.00	612.75	580.50	548.25	516.00
SA-SRO	Sub-router	324.50	295.00	280.25	265.50	250.75	236.00
SA-TRK	Tracker	819.50	745.00	707.75	670.50	633.25	596.00
SA-UKN	Universal Key, No Button	87.00	79.00	75.00	71.00	67.00	63.25

Guardian Server		
SAG-HW-50-TW	SA-Guardian "Micro server" Tower H/W for 50 doors	1,599.00
SAG-HW-100-TW	SA-Guardian "Mini server" Tower H/W for100 doors	2,499.00
SAG-HW-250-RM	SA-Guardian "Feather server" Rackmount H/W for 250 doors	3,500.00
SAG-HW-500-RM	SA-Guardian "Lite server" Rackmount H/W for 500 doors	4,995.00
SAG-HW-1K-RM	SA-Guardian "Standard server" Rackmount H/W for 1K doors	6,550.00
SAG-HW-2K-RM	SA-Guardian "Fort server" Rackmount H/W for 2K doors	8,150.00
SAG-HW-4K-RM	SA-Guardian "Castle server" Rackmount single node H/W up to 4K doors	9,550.00
SAG-HW-15K-RM	SA-Guardian "Knox server" Rackmount dual node H/W up to 15K doors	29,250.00

Guardian Software		
SAG-AS-MICRO	SA-Guardian software- "Micro" -Perpetual license. Up to 50 doors. Oracle-XE, Includes 2 NUL Operator GUI. Standard reports.	1,200.00
SAG-AS-MINI	SA-Guardian software- "Mini" -Perpetual license. Up to 100 doors. Oracle-XE, Includes 2 NUL Operator GUI. Standard reports.	1,795.00
SAG-AS-FEATHER	SA-Guardian software- "Feather" -Perpetual license. Up to 250 doors. Oracle-XE, Includes 2 NUL Operator GUI. Standard reports.	2,350.00
SAG-AS-LITE	SA-Guardian software- "Lite" -Perpetual license. Up to 500 doors. Oracle-XE, Includes 2 NUL Operator GUI. Standard reports.	2,950.00
SAG-AS-STANDARD	SA-Guardian software- "Standard" -Perpetual license. Up to 1000 doors. Oracle-XE, Includes 2 NUL Operator GUI. Standard reports.	4,250.00
SAG-AS-FORT	SA-Guardian software- "Fort" -Perpetual license. Up to 2,000 doors. Oracle-XE, Includes 2 NUL Operator GUI. Standard reports.	5,500.00
SAG-AS-CASTLE	SA-Guardian application software- Castle- Perpetual license. Up to 4000 doors. Oracle-SE2, Include 2 NUL Operator GUI. Standard reports.	9,995.00
SAG-AS-KNOX	SA-Guardian application software- Knox- Perpetual license. Up to 15,000 doors. Oracle-SE2, Include 2 NUL Operator GUI. Standard reports.	17,995.00
SAG-OPR-GUI	SA-Guardian Operator GUI (5 pack NUL)	1,500.00
SAG-WEBSRVIF	Web-services API Interface software module	5,500.00
SAG-BULKUPLD	Bulk upload module. User and Facility	3,600.00
SAG-SSO-SLAM	SLAM single sign-on	4,995.00

Optional Service & Training		
SA-SRV-SRVINSTALL	Initial server hardware and software setup - VLAN, Firewall, Connectivity, CRON tasks, NAS backup (Est. 24 Hrs.)	$154/hr
SA-SRV-ISET	Initial system setup - process owner, best practices (Est. 40 Hrs.)	$154/hr
SA-SRV-SW	System integration consulting, incl. web services. (Est. 90 Hrs.)	$194/hr
SA-SRV-PM	Project management and coordination (Est. 120 Hrs.)	$194/hr
SA-TRN-LK1	Training: Locksmith training-1 (basic) CDR, MDR, PHR, PWR (6 Hrs., Group of 3)	1,620.00
SA-TRN-LK2	Training: Locksmith training-1 advanced Lock configuration options (6 Hrs., Group of 3)	1,620.00
SA-TRN-SW1	SA-Guardian operator training (8 Hrs., Group of 4)	2,880.00
SA-TRN-SW2	SA-Guardian operator refresher training. Pre-requisite SA-TRN-SW1 (4 Hrs., Group of 4)	1,440.00
SA-TRN-SW3	SA-Guardian advanced operator training (8 Hrs., Group of 4)	2,880.00
SA-TRN-SW4	SA-Guardian interface programming training (3 sessions of 6 Hrs. each, Group of 3)	4,860.00
SA-TRN-SW5	Training: SA-Guardian Power user, Process-owner (site, naming conventions, facility model, custom fields, device config parameters, facility model parameters, sys-engineer) (2 sessions of 6 Hrs. each, Group of 3)	3,240.00
SA-EXT-SOFT1K	Post-warranty Annual Extended Software Support and Update including device firmware up to 1,000 locks system (including up to 20 Hrs technical phone support and up to 10 Hrs software engineering effort to deploy server software updates or patches). Applicable for standard server software product line items; does not cover software customization or integration. Requires internet connectivity to onsite remote support PC.	3,660.00
SA-EXT-SOFT4K	Post-warranty Annual Extended Software Support and Update including device firmware up to 4,000 locks system (including up to 30 Hrs technical phone support and up to 15 Hrs software engineering effort to deploy server software updates or patches). Applicable for standard server software product line items; does not cover software customization or integration. Requires internet connectivity to onsite remote support PC.	6,680.00
SA-EXTWAR	Post-warranty Annual Extended Hardware Support. Extends the company's hardware warranty policy for an additional year.	2% of installed hardware

SecureALL Price List*

* Volume price discounts apply to total unit quantity ordered within a category, i.e. locking hardware

**Escalation cost is built in at a not to exceed 5% per year. This is formatted to show a not to exceed price. Price may be less depending on the CPI, check with vendor for annual escalation

*** Standard terms are net 30. Discounts are available: 2% net 10; 1% net 20

		Year 2 of Contract September 2018 - August 2019					
Locking Hardware		< 100	100 - 250	251 - 500	501 - 1000	1001 - 5000	> 5001
SA-CDR	Cylindrical Door Reader	779.50	708.75	673.25	637.75	602.50	567.00
SA-CRR	Cylindrical Restroom (Privacy) Reader	821.50	750.75	715.25	679.75	644.50	609.00
SA-MDR	Mortise Door Reader	860.50	782.25	743.00	704.00	665.00	625.75
SA-MRR	Mortise Restroom (Privacy) Reader	902.50	824.25	785.00	746.00	707.00	667.75
SA-ODR	Onity Door Reader Retrofit Kit	634.25	576.50	547.50	518.50	489.75	461.00
SA-OGD	Dual Outside Gate (Garage) Reader - Long Range	1472.50	1338.75	1271.75	1204.75	1138.00	1071.00
SA-OGR	Outside Gate (Garage) Reader - Long Range	895.00	813.75	773.00	732.25	691.50	651.00
SA-OPR	Onity Panic Hardware Reader Retrofit Kit	749.75	681.50	647.25	613.00	579.00	545.00
SA-PCD	Passage Cylindrical Door Reader	571.75	519.75	493.75	467.75	441.75	415.75
SA-PMD	Passage Mortise Door Reader	652.50	593.25	563.50	534.00	504.25	474.50
SA-PHM	Panic Hardware Mortise Device	N/A	N/A	N/A	N/A	N/A	N/A
SA-PHR	Panic Hardware Rim Device (Von Duprin 98/99) Retrofit Kit	1077.00	979.00	892.50	849.00	806.00	762.50
SA-PSR	Point of Sale Reader	837.25	761.25	723.00	685.00	647.00	609.00
SA-PWD	Dual Panic Wall Reader	1414.75	1286.25	1221.75	1157.50	1093.25	1029.00
SA-PWR	Panic Wall Reader	837.25	761.25	723.00	685.00	647.00	609.00

Option Adders		< 100	100 - 250	251 - 500	501 - 1000	1001 - 5000	> 5001
C	SFIC Keyway Included	115.50	105.00	99.75	94.50	89.25	84.00
D	Dual Proximity and Smartcard Reader	173.25	157.50	149.50	141.75	133.75	126.00
G	Standard Falcon Cylindrical Keyway for PHR	115.50	105.00	99.75	94.50	89.25	84.00
H	Handle to Accommodate SFIC (core customer supplied)	28.75	26.25	25.00	23.50	22.25	21.00
K	10 Key Pushbutton	99.75	94.50	91.75	89.25	86.50	81.00
O	Outdoor Weatherization	115.50	105.00	99.75	94.50	89.25	84.00
P	Proximity Card Reader	115.50	105.00	99.75	94.50	89.25	84.00
S	Smartcard Reader	115.50	105.00	99.75	94.50	89.25	84.00

Ancillary Equipment		< 100	100 - 250	251 - 500	501 - 1000	1001 - 5000	> 5001
SA-APS	Auxiliary Power Supply	519.75					
SA-ITK	Installation Tool Kit	414.75					
SA-LST	Deadlatch Sensor Tester	309.75					
SA-SAT	Site Audit Tool Kit	1044.75					
SA-UKR	Universal Key Reader	414.75					
SA-LOC	Locator	623.70	567.00	538.50	510.25	482.00	453.50
SA-ROU	Router	745.00	677.25	643.50	609.50	575.50	541.75
SA-SRO	Sub-router	340.75	309.75	294.25	278.75	263.25	247.75
SA-TRK	Tracker	860.50	782.25	743.00	704.00	664.75	625.75
SA-UKN	Universal Key, No Button	91.25	83.00	78.75	74.50	70.25	66.50

Guardian Server		
SAG-HW-50-TW	SA-Guardian "Micro server" Tower H/W for 50 doors	1,679.00
SAG-HW-100-TW	SA-Guardian "Mini server" Tower H/W for100 doors	2,624.00
SAG-HW-250-RM	SA-Guardian "Feather server" Rackmount H/W for 250 doors	3,675.00
SAG-HW-500-RM	SA-Guardian "Lite server" Rackmount H/W for 500 doors	5,244.75
SAG-HW-1K-RM	SA-Guardian "Standard server" Rackmount H/W for 1K doors	6,877.50
SAG-HW-2K-RM	SA-Guardian "Fort server" Rackmount H/W for 2K doors	8,557.50
SAG-HW-4K-RM	SA-Guardian "Castle server" Rackmount single node H/W up to 4K doors	10,027.50
SAG-HW-15K-RM	SA-Guardian "Knox server" Rackmount dual node H/W up to 15K doors	30,712.50

Guardian Software		
SAG-AS-MICRO	SA-Guardian software- "Micro" -Perpetual license. Up to 50 doors. Oracle-XE, Includes 2 NUL Operator GUI. Standard reports.	1,260.00
SAG-AS-MINI	SA-Guardian software- "Mini" -Perpetual license. Up to 100 doors. Oracle-XE, Includes 2 NUL Operator GUI. Standard reports.	1,884.75
SAG-AS-FEATHER	SA-Guardian software- "Feather" -Perpetual license. Up to 250 doors. Oracle-XE, Includes 2 NUL Operator GUI. Standard reports.	2,467.50
SAG-AS-LITE	SA-Guardian software- "Lite" -Perpetual license. Up to 500 doors. Oracle-XE, Includes 2 NUL Operator GUI. Standard reports.	3,097.50
SAG-AS-STANDARD	SA-Guardian software- "Standard" -Perpetual license. Up to 1000 doors. Oracle-XE, Includes 2 NUL Operator GUI. Standard reports.	4,462.50
SAG-AS-FORT	SA-Guardian software- "Fort" -Perpetual license. Up to 2,000 doors. Oracle-XE, Includes 2 NUL Operator GUI. Standard reports.	5,775.00
SAG-AS-CASTLE	SA-Guardian application software- Castle- Perpetual license. Up to 4000 doors. Oracle-SE2, Include 2 NUL Operator GUI. Standard reports.	10,494.75
SAG-AS-KNOX	SA-Guardian application software- Knox- Perpetual license. Up to 15,000 doors. Oracle-SE2, Include 2 NUL Operator GUI. Standard reports.	18,894.75
SAG-OPR-GUI	SA-Guardian Operator GUI (5 pack NUL)	1,575.00
SAG-WEBSRVIF	Web-services API Interface software module	5,775.00
SAG-BULKUPLD	Bulk upload module. User and Facility	3,780.00
SAG-SSO-SLAM	SLAM single sign-on	5,244.75

Optional Service & Training		
SA-SRV-SRVINSTALL	Initial server hardware and software setup - VLAN, Firewall, Connectivity, CRON tasks, NAS backup (Est. 24 Hrs.)	$161.70/hr
SA-SRV-ISET	Initial system setup - process owner, best practices (Est. 40 Hrs.)	$161.70/hr
SA-SRV-SW	System integration consulting, incl. web services. (Est. 90 Hrs.)	$203.70/hr
SA-SRV-PM	Project management and coordination (Est. 120 Hrs.)	$203.70/hr
SA-TRN-LK1	Training: Locksmith training-1 (basic) CDR, MDR, PHR, PWR (6 Hrs., Group of 3)	1,701.00
SA-TRN-LK2	Training: Locksmith training-1 advanced Lock configuration options (6 Hrs., Group of 3)	1,701.00
SA-TRN-SW1	SA-Guardian operator training (8 Hrs., Group of 4)	3,024.00
SA-TRN-SW2	SA-Guardian operator refresher training. Pre-requisite SA-TRN-SW1 (4 Hrs., Group of 4)	1,512.00
SA-TRN-SW3	SA-Guardian advanced operator training (8 Hrs., Group of 4)	3,024.00
SA-TRN-SW4	SA-Guardian interface programming training (3 sessions of 6 Hrs. each, Group of 3)	5,103.00
SA-TRN-SW5	Training: SA-Guardian Power user, Process-owner (site, naming conventions, facility model, custom fields, device config parameters, facility model parameters, sys-engineer) (2 sessions of 6 Hrs. each, Group of 3)	3,402.00
SA-EXT-SOFT1K	Post-warranty Annual Extended Software Support and Update including device firmware up to 1,000 locks system (including up to 20 Hrs technical phone support and up to 10 Hrs software engineering effort to deploy server software updates or patches). Applicable for standard server software product line items; does not cover software customization or integration. Requires internet connectivity to onsite remote support PC.	3,843.00
SA-EXT-SOFT4K	Post-warranty Annual Extended Software Support and Update including device firmware up to 4,000 locks system (including up to 30 Hrs technical phone support and up to 15 Hrs software engineering effort to deploy server software updates or patches). Applicable for standard server software product line items; does not cover software customization or integration. Requires internet connectivity to onsite remote support PC.	7,014.00
SA-EXTWAR	Post-warranty Annual Extended Hardware Support. Extends the company's hardware warranty policy for an additional year.	2.1% of installed hardware

SecureALL Price List*

* Volume price discounts apply to total unit quantity ordered within a category, i.e. locking hardware

**Escalation cost is built in at a not to exceed 5% per year. This is formatted to show a not to exceed price. Price may be less depending on the CPI, check with vendor for annual escalation

*** Standard terms are net 30. Discounts are available: 2% net 10; 1% net 20

		Year 3 of Contract September 2019 - August 2020					
Locking Hardware		< 100	100 - 250	251 - 500	501 - 1000	1001 - 5000	> 5001
SA-CDR	Cylindrical Door Reader	818.50	744.00	707.00	669.50	632.50	595.25
SA-CRR	Cylindrical Restroom (Privacy) Reader	862.50	788.25	751.00	713.75	676.75	639.50
SA-MDR	Mortise Door Reader	903.50	821.25	780.00	739.00	698.25	657.00
SA-MRR	Mortise Restroom (Privacy) Reader	947.50	865.50	824.25	783.25	742.25	701.00
SA-ODR	Onity Door Reader Retrofit Kit	666.00	605.25	574.75	544.25	514.25	484.00
SA-OGD	Dual Outside Gate (Garage) Reader - Long Range	1546.00	1405.50	1335.25	1265.00	1195.00	1124.50
SA-OGR	Outside Gate (Garage) Reader - Long Range	939.75	854.50	811.50	768.75	726.00	683.50
SA-OPR	Onity Panic Hardware Reader Retrofit Kit	787.25	715.50	679.50	643.50	608.00	572.25
SA-PCD	Passage Cylindrical Door Reader	600.25	545.75	518.50	491.00	463.75	436.50
SA-PMD	Passage Mortise Door Reader	685.00	622.75	591.50	560.50	529.50	498.25
SA-PHM	Panic Hardware Mortise Device	N/A	N/A	N/A	N/A	N/A	N/A
SA-PHR	Panic Hardware Rim Device (Von Duprin 98/99) Retrofit Kit	1130.75	1028.00	937.00	891.50	846.25	800.50
SA-PSR	Point of Sale Reader	879.00	799.25	759.00	719.25	679.25	639.50
SA-PWD	Dual Panic Wall Reader	1485.50	1350.50	1282.75	1215.25	1148.00	1080.50
SA-PWR	Panic Wall Reader	879.00	799.25	759.00	719.25	679.25	639.50

Option Adders		< 100	100 - 250	251 - 500	501 - 1000	1001 - 5000	> 5001
C	SFIC Keyway Included	121.25	110.25	104.75	99.25	93.75	88.00
D	Dual Proximity and Smartcard Reader	182.00	165.25	157.00	148.50	140.50	132.25
G	Standard Falcon Cylindrical Keyway for PHR	121.25	110.25	104.75	99.25	93.75	88.00
H	Handle to Accommodate SFIC (core customer supplied)	30.00	27.50	26.25	24.50	23.25	22.00
K	10 Key Pushbutton	104.75	99.25	96.25	93.75	90.75	85.25
O	Outdoor Weatherization	121.25	110.25	104.75	99.25	93.75	88.00
P	Proximity Card Reader	121.25	110.25	104.75	99.25	93.75	88.00
S	Smartcard Reader	121.25	110.25	104.75	99.25	93.75	88.00

Ancillary Equipment		< 100	100 - 250	251 - 500	501 - 1000	1001 - 5000	> 5001
SA-APS	Auxiliary Power Supply	545.75					
SA-ITK	Installation Tool Kit	435.50					
SA-LST	Deadlatch Sensor Tester	325.25					
SA-SAT	Site Audit Tool Kit	1097.00					
SA-UKR	Universal Key Reader	435.50					
SA-LOC	Locator	654.75	595.25	565.50	535.75	506.00	476.00
SA-ROU	Router	782.25	711.00	675.50	640.00	604.25	568.75
SA-SRO	Sub-router	357.75	325.25	309.00	292.50	276.25	260.00
SA-TRK	Tracker	903.50	821.25	780.00	739.00	698.00	657.00
SA-UKN	Universal Key, No Button	95.75	87.00	82.50	78.25	73.75	69.75

Guardian Server		
SAG-HW-50-TW	SA-Guardian "Micro server" Tower H/W for 50 doors	1,763.00
SAG-HW-100-TW	SA-Guardian "Mini server" Tower H/W for100 doors	2,755.25
SAG-HW-250-RM	SA-Guardian "Feather server" Rackmount H/W for 250 doors	3,858.75
SAG-HW-500-RM	SA-Guardian "Lite server" Rackmount H/W for 500 doors	5,507.00
SAG-HW-1K-RM	SA-Guardian "Standard server" Rackmount H/W for 1K doors	7,221.25
SAG-HW-2K-RM	SA-Guardian "Fort server" Rackmount H/W for 2K doors	8,985.50
SAG-HW-4K-RM	SA-Guardian "Castle server" Rackmount single node H/W up to 4K doors	10,528.75
SAG-HW-15K-RM	SA-Guardian "Knox server" Rackmount dual node H/W up to 15K doors	32,248.00

Guardian Software		
SAG-AS-MICRO	SA-Guardian software- "Micro" -Perpetual license. Up to 50 doors. Oracle-XE, Includes 2 NUL Operator GUI. Standard reports.	1,323.00
SAG-AS-MINI	SA-Guardian software- "Mini" -Perpetual license. Up to 100 doors. Oracle-XE, Includes 2 NUL Operator GUI. Standard reports.	1,979.00
SAG-AS-FEATHER	SA-Guardian software- "Feather" -Perpetual license. Up to 250 doors. Oracle-XE, Includes 2 NUL Operator GUI. Standard reports.	2,591.00
SAG-AS-LITE	SA-Guardian software- "Lite" -Perpetual license. Up to 500 doors. Oracle-XE, Includes 2 NUL Operator GUI. Standard reports.	3,252.25
SAG-AS-STANDARD	SA-Guardian software- "Standard" -Perpetual license. Up to 1000 doors. Oracle-XE, Includes 2 NUL Operator GUI. Standard reports.	4,685.50
SAG-AS-FORT	SA-Guardian software- "Fort" -Perpetual license. Up to 2,000 doors. Oracle-XE, Includes 2 NUL Operator GUI. Standard reports.	6,063.75
SAG-AS-CASTLE	SA-Guardian application software- Castle- Perpetual license. Up to 4000 doors. Oracle-SE2, Include 2 NUL Operator GUI. Standard reports.	11,019.50
SAG-AS-KNOX	SA-Guardian application software- Knox- Perpetual license. Up to 15,000 doors. Oracle-SE2, Include 2 NUL Operator GUI. Standard reports.	19,839.50
SAG-OPR-GUI	SA-Guardian Operator GUI (5 pack NUL)	1,653.75
SAG-WEBSRVIF	Web-services API Interface software module	6,063.75
SAG-BULKUPLD	Bulk upload module. User and Facility	3,969.00
SAG-SSO-SLAM	SLAM single sign-on	5,507.00

Optional Service & Training		
SA-SRV-SRVINSTALL	Initial server hardware and software setup - VLAN, Firewall, Connectivity, CRON tasks, NAS backup (Est. 24 Hrs.)	$169.79/hr
SA-SRV-ISET	Initial system setup - process owner, best practices (Est. 40 Hrs.)	$169.79/hr
SA-SRV-SW	System integration consulting, incl. web services. (Est. 90 Hrs.)	$213.89/hr
SA-SRV-PM	Project management and coordination (Est. 120 Hrs.)	$213.89/hr
SA-TRN-LK1	Training: Locksmith training-1 (basic) CDR, MDR, PHR, PWR (6 Hrs., Group of 3)	1,786.00
SA-TRN-LK2	Training: Locksmith training-1 advanced Lock configuration options (6 Hrs., Group of 3)	1,786.00
SA-TRN-SW1	SA-Guardian operator training (8 Hrs., Group of 4)	3,175.00
SA-TRN-SW2	SA-Guardian operator refresher training. Pre-requisite SA-TRN-SW1 (4 Hrs., Group of 4)	1,587.50
SA-TRN-SW3	SA-Guardian advanced operator training (8 Hrs., Group of 4)	3,175.00
SA-TRN-SW4	SA-Guardian interface programming training (3 sessions of 6 Hrs. each, Group of 3)	5,358.00
SA-TRN-SW5	Training: SA-Guardian Power user, Process-owner (site, naming conventions, facility model, custom fields, device config parameters, facility model parameters, sys-engineer) (2 sessions of 6 Hrs. each, Group of 3)	3,572.00
SA-EXT-SOFT1K	Post-warranty Annual Extended Software Support and Update including device firmware up to 1,000 locks system (including up to 20 Hrs technical phone support and up to 10 Hrs software engineering effort to deploy server software updates or patches). Applicable for standard server software product line items; does not cover software customization or integration. Requires internet connectivity to onsite remote support PC.	4,035.00
SA-EXT-SOFT4K	Post-warranty Annual Extended Software Support and Update including device firmware up to 4,000 locks system (including up to 30 Hrs technical phone support and up to 15 Hrs software engineering effort to deploy server software updates or patches). Applicable for standard server software product line items; does not cover software customization or integration. Requires internet connectivity to onsite remote support PC.	7,364.75
SA-EXTWAR	Post-warranty Annual Extended Hardware Support. Extends the company's hardware warranty policy for an additional year.	2.21% of installed hardware

Addendum #5 8/1/17

SecureALL Product Data Sheets

1) SA-CDR Cylindrical Door Reader
2) SA-CDR Cylindrical Door Reader w/Card Read
3) SA-GSW Guardian Software
4) SA-MDR Mortise Door Reader
5) SA-MDR Mortise Door Reader w/Card Read
6) SA-PHR Panic Hardware Reader, Retrofit Kit for Von Duprin 98/99 Rim Hardware
7) SA-PWR Panic Wall Reader
8) SA-ROU Router (Access Point)
9) SA-TRK Tracker

SECUREALL SECURITY REINVENTED℠

Cylindrical Door Reader SA-CDR

Electrical specifications

Users	Up to 70,000
Audit Trail	6 mos. data stored in server, typical
Credential Verification Time	< 50ms
Visual/Audible Interface	LED and audio beeper
System Interface	SA-*Guardian* Application Server
Power Supply	3 or 4 standard AA alkaline batteries; depends on keying option
Battery Life	4 years, typical
Exterior Operating Temperature	-10° C to +70° C or +14° F to +158° F
Interior Operating Temperature	-10° C to +55° C or +14° F to +131° F
Certifications/Compliance	FCC Part 15 B&C
Reader Technology	Hands-free, wireless
Reader Frequency	2.4 GHz
Reader Range	1" to 30 ft, programmable
Communication Security	PKI, AES-128
Encryption Keys	Device specific, customer controlled
Wireless Communication Protocol	Proprietary: Extreme low power (ELP) protocol & 802.15.4
Reader/Router Handshake	Automatic
Firmware Updates	PKI; over-the-air
Electrical Warranty	2 years

Features & Benefits

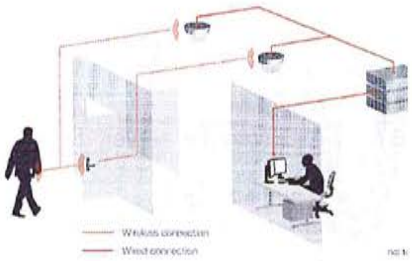
- **Hands-free, multi-distance access**
- **Long range, hands-free asset tracking**
- **Real-time, extreme low power communication => long battery life**
- **All access decisions at the door; does not require server link**
- **Multi-layer hard encryption: PKI +AES**
- **Device specific encryption keys, controlled by system owner**
- **Remote & local lockdown**
- **Over-the-air firmware upgrades**
- **Manual & programmable office mode**
- **Integrated door ajar and tamper sensor**
- **Remote unlock**
- **No software or lease licenses**

Mechanical specifications

Handing	Universal, non-handed; ADA compliant
Certifications/Compliance	ANSI/BHMA A156.2 Grade 1; UL10c-3 hour
Door Thickness	1-5/8" to 2"
Backset	2-3/4"
Latches	Stainless steel, 17/32" throw
Lever Design	Sentinel
Lever Functionality	Clutched (free wheeling)
Strikes	ASA strike
Keying	Hands-free U-Key™
Function	Passage, privacy, entry, classroom, storeroom; other functions available upon request
Case Material	Satin stainless steel (630)
Dimensions	O/S 9-3/8" x 3-1/8" x 27/32"
Vandal Protection	Integrated tamper sensors
Door Ajar Alarm	Integrated deadlatch sensor
Mechanical Warranty	2 years

Cylindrical Door Reader SA-CDR

How it works



SA-CDR Options

Keying	In addition to U-Key™ operation: 10-key pushbutton; BEST or SARGENT SFIC keyway; Proximity and Smartcard; Bluetooth
Lever Design	Quest
Lever Functionality	Non-clutched
Finish	Satin brass (606) Oil rubbed bronze (613) Satin nickel (619) Satin chrome (626)
Strike	T-Strike, Full-lip
Outdoor Usage	Weatherized
Saniguard	Antimicrobial coating

Frequently asked questions

1. **Do locks come with access options other than a U-Key™?** This lock supports SecureALL U-Key™, Proximity and Smartcard credentials. Options are available to add a cost effective 10-button keypad and/or a mechanical (SFIC) key cylinder.
2. **Where does access control information reside in the system?** The SA *Guardian* automatically sends this information to each applicable lock. The lock is then fully capable of making access control decisions without going back to the Server. As locks are battery operated, doors will continue to function, even in the event of a power failure.
3. **What is tracking capability:** Each lock has the built-in ability to automatically track a hands-free U-Key™ (person or asset) as it passes by the door. It can optionally be turned on.
4. **How many lock units can be controlled by a single router?** There is no limit to the number of doors that can be controlled by a single router (limited only by building construction) and no licenses are required.
5. **Can a U-Key™ unlock a door when approached from inside?** SecureALL locks are designed to know whether a U-Key™ is located inside or outside a room. Therefore, a door can never unlock by accident when approached from inside, i.e. looking though a door peephole.
6. **Does the system send a low battery alarm?** When batteries in any of the system components reach a programmed minimum level, an individual designated by the system administrator is notified, via the client screen, email or text message, that batteries must be changed.
7. **What level of encryption is incorporated in the system?** SecureALL utilizes multiple levels of encryption (PKI and AES), first to ensure that any equipment being added to a customer's system is genuine, and then to guarantee that end-to-end communication between all layers is secure at the highest possible level. Customers have complete control over encryption keys.
8. **Can a door be unlocked if the batteries are dead?** An auxiliary power supply is available that energizes the door lock, allowing an authorized U-Key™ entrance to a room.
9. **Lock installation tools?** Ordinary workbench tools; no special programmer or cable.

SECUREALL SECURITY REINVENTED℠

Cylindrical Door Reader SA-CDR w/Card Option

Features & Benefits

- **Hands-free, multi-distance access**
- **Proximity and Smartcard**
- **Long range, hands-free asset tracking**
- **Real-time, extreme low power communication => long battery life**
- **All access decisions at the door; does not require server link**
- **Multi-layer hard encryption: PKI +AES**
- **Device specific encryption keys, controlled by system owner**
- **Remote & local lockdown**
- **Over-the-air firmware upgrades**
- **Manual & programmable office mode**
- **Integrated door ajar and tamper sensor**
- **Remote unlock**
- **No software or lease licenses**

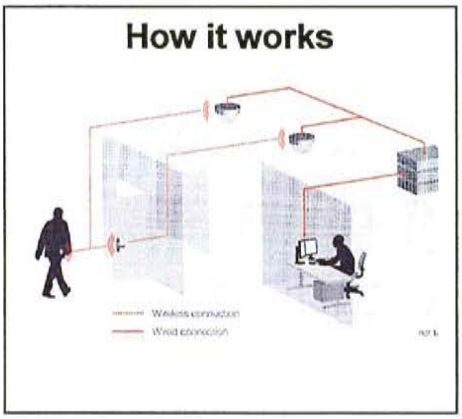
Electrical specifications

Users	Up to 70,000
Audit Trail	6 mos. data stored in server, typical
Credential Verification Time	< 50ms
Visual/Audible Interface	LED and audio beeper
System Interface	SA-*Guardian* Application Server
Power Supply	4 standard AA alkaline batteries
Battery Life	4 years, typical ; 100K openings
Exterior Operating Temperature	-10° C to +70° C or +14° F to +158° F
Interior Operating Temperature	-10° C to +55° C or +14° F to +131° F
Certifications/Compliance	FCC Part 15 B&C
Reader Technology: Hands free UKey: Contactless Smartcard: Bluetooth /Smartphone:	 Hands-free, wireless, PKI, AES ISO 14443, sector cryptography Bluetooth (BLE)
Reader Frequency	2.4 GHz and 13.56 MHz
Reader Range	UKey: 1" to 30 ft, programmable Card and BLE: 1"
Communication Security	PKI, AES-128
Encryption Keys	Device specific, customer controlled
Wireless Communication Protocol	Proprietary: Extreme low power (ELP) protocol & 802.15.4; 14443
Reader/Router Handshake	Automatic
Firmware Updates	PKI; over-the-air
Electrical Warranty	2 years

Mechanical specifications

Handing	Universal, non-handed; ADA compliant
Certifications/Compliance	ANSI/BHMA A156.2 Grade 1; UL10c-3 hour
Door Thickness	1-5/8" to 2"
Backset	2-3/4"
Latches	Stainless steel, 17/32" throw
Lever Design	Sentinel
Lever Functionality	Clutched (free wheeling)
Strikes	ASA strike
Keying	Hands-free U-Key™, Card, BLE
Function	Passage, privacy, entry, classroom, storeroom; other functions available upon request
Case Material	Satin stainless steel (630)
Dimensions	O/S 9-3/8" x 3-1/8" x 27/32"
Vandal Protection	Integrated tamper sensors
Door Ajar Alarm	Integrated deadlatch sensor
Mechanical Warranty	2 years

Cylindrical Door Reader SA-CDR w/Card Option



SA-CDR Options

Keying	In addition to U-Key™ operation: 10-key pushbutton; BEST or SARGENT SFIC keyway
Lever Design	Quest
Lever Functionality	Non-clutched
Finish	Satin brass (606) Oil rubbed bronze (613) Satin nickel (619) Satin chrome (626)
Strike	T-Strike, Full-lip
Outdoor Usage	Weatherized
Saniguard	Antimicrobial coating

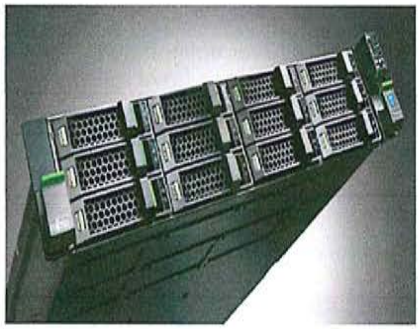
Frequently asked questions

1. **Do locks come with access options other than a U-Key™?** This lock supports SecureALL U-Key™, Proximity and Smartcard credentials. Options are available to add a cost effective 10-button keypad and/or a mechanical (SFIC) key cylinder.
2. **Where does access control information reside in the system?** The SA *Guardian* automatically sends this information to each applicable lock. The lock is then fully capable of making access control decisions without going back to the Server. As locks are battery operated, doors will continue to function, even in the event of a power failure.
3. **What is tracking capability:** Each lock has the built-in ability to automatically track a hands-free U-Key™ (person or asset) as it passes by the door. It can optionally be turned on.
4. **How many lock units can be controlled by a single router?** There is no limit to the number of doors that can be controlled by a single router (limited only by building construction) and no licenses are required.
5. **Can a U-Key™ unlock a door when approached from inside?** SecureALL locks are designed to know whether a U-Key™ is located inside or outside a room. Therefore, a door can never unlock by accident when approached from inside, i.e. looking though a door peephole.
6. **Does the system send a low battery alarm?** When batteries in any of the system components reach a programmed minimum level, an individual designated by the system administrator is notified, via the client screen, email or text message, that batteries must be changed.
7. **What level of encryption is incorporated in the system?** SecureALL utilizes multiple levels of encryption (PKI and AES), first to ensure that any equipment being added to a customer's system is genuine, and then to guarantee that end-to-end communication between all layers is secure at the highest possible level. Customers have complete control over encryption keys.
8. **Can a door be unlocked if the batteries are dead?** An auxiliary power supply is available that energizes the door lock, allowing an authorized U-Key™ entrance to a room.
9. **Lock installation tools?** Ordinary workbench tools; no special programmer or cable.

SECUREALL SECURITY REINVENTED℠

Guardian Software SA-GSW

(comes installed on a SecureALL supplied server)



Server specifications

Package	Laptop, rack mount w/single power supply, or rack mount with dual power supply
Rack Mount Dimensions	19.85" x 17.2" x 1.7"
Rack Mount Power Supply	100-240 VAC / 400W
CPU	1 - 2 Intel Xeon E5-2600
Memory	32 - 128 GB
Mass Storage	SSD and HDD: RAID-1
Remote Management	IPMI 1.5/2.0 dedicated LAN
LAN Interfaces	2 x 1000BASE-T, RJ45
Operating Temperature	+10°C to +35°C
Operating Humidity	8 - 90%, non-condensing
Operating System	Linux/CentOS
Application Server	JBoss
Application Software	SA *Guardian*

Features & Benefits

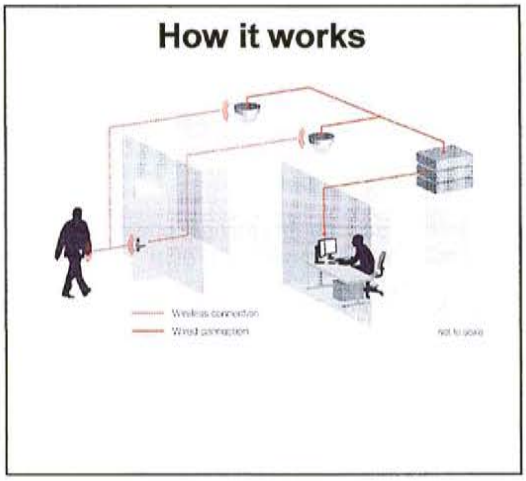
- **Turn key - ready to use system**
- **End-to-end hard encryption**
- **No backdoor - customer owns the encryption keys**
- **Easy to set up and maintain**
- **Server is data repository only; locks have autonomous control over accessibility**
- **No risk of compromised site encryption key**
- **Domains allow flexible and cooperative multi-department use**
- **Lowest Total Cost of Ownership**
- **Multi-featured, not simple access control**
- **System capability can be expanded as users and requirements grow**

System specifications

Size	1K, 5K, 10K, 20K, 70K doors
U-Key™ Users	Up to 70,000
Concurrent GUI Users	≤ 12
Access Groups	Up to 10,000, each with up to 500 room schedules
User Membership of Access Groups	Up to 100 memberships/user
U-Key™ Access Levels	5 levels available. The highest level is assigned to "first responders," who have access even during lockdown
GUI Encryption	SSL
Device Communication	PKI and AES
Audit Trail	3 months of data stored
Door Activation Distance	Programmable from 20% to 300% of standard opening distance (3')
Client Operating System	Windows

Guardian Software SA-GSW

How it works



System functionality

New Device Join	PKI cryptographic acceptance
Encryption Keys	Each device has separate PKI and AES encryption key; user controlled
U-Key™ Encryption	Separate key per door
Remote Lockdown	By room, floor, building, campus, or pre-defined door set
Local Lockdown	At a door
"Reflex" Lockdown	Automatically locks down a building when multiple local lockdowns are initiated within a defined time period
Partitioning of Campus	Each administrator controls only a specific part of the campus
Role Management	Collection of user defined action privileges. User can have multiple roles
Support Isolated Secured Network	Router connected to server via VLAN
Door Unlock	Local (with U-Key™) and remote
Asset and People Tracking	Utilizes door locks and/or tracker
Integration With Other Enterprise Systems	Web-services compliant interface
Security Watch Window	Puts U-Key™ user's picture on a monitor for extra validation

Frequently asked questions

1. **Do customers have to purchase server hardware?** SecureALL provides a turnkey, prebuilt server with the *Guardian* software ready to use. Servers are sized for a customer's specific needs. The server can be field upgraded as capacity requirements increase.
2. **Where does access control information reside in the system?** The server automatically downloads this information to each applicable lock. The lock is then fully capable of making access control decisions without going back to the server. As locks are battery operated, doors will continue to function, even in the event of a power failure.
3. **Does SecureALL have a master account for access into a deployed server?** No, customers are in complete control of users who can log into the system and their operational and domain privileges. Customers have the option of creating their own private PKI keys, not known to SecureALL, thus ensuring no backdoor entry.
4. **Can one server handle multiple campuses?** Yes, the only requisite is that the LAN connecting the SecureALL routers be configured to provide a low latency communication link with the server. Client PCs can also be deployed across multiple campuses.
5. **Can the server be located in the "cloud?"** For security and logistics reasons, customers should resist the urge to place their security system server outside their physical control. However, as long as a customer has the necessary network tunneling (quality of service and firewall protection connecting the server, routers and client PC), the *Guardian* system can be deployed in many different topologies.

SECUREALL SECURITY REINVENTED℠

Mortise Door Reader SA-MDR

Electrical specifications

Users	Up to 70,000
Audit Trail	6 mos. data stored in server, typical
Credential Verification Time	< 50ms
Visual/Audible Interface	LED and audio beeper
System Interface	SA-*Guardian* Application Server
Power Supply	3 or 4 standard AA alkaline batteries; depends on keying option
Battery Life	4 years, typical
Exterior Operating Temperature	-10° C to +70° C or +14° F to +158° F
Interior Operating Temperature	-10° C to +55° C or +14° F to +131° F
Certifications/Compliance	FCC Part 15 B&C
Reader Technology	Hands-free, wireless
Reader Frequency	2.4 GHz
Reader Range	1" to 30 ft, programmable
Communication Security	PKI, AES-128
Encryption Keys	Device specific, customer controlled
Wireless Communication Protocol	Proprietary: Extreme low power (ELP) protocol & 802.15.4
Reader/Router Handshake	Automatic
Firmware Updates	PKI; over-the-air
Electrical Warranty	2 years

Features & Benefits

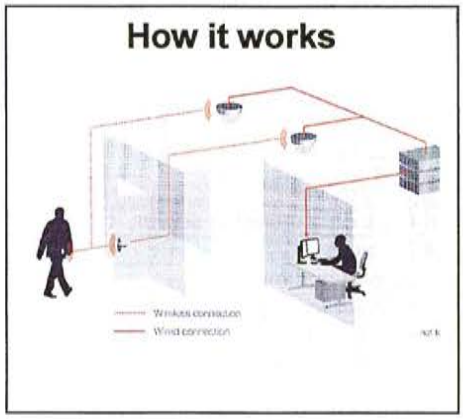
- **Hands-free, multi-distance access**
- **Long range, hands-free asset tracking**
- **Real-time, extreme low power communication => long battery life**
- **All access decisions at the door; does not require server link**
- **Multi-layer hard encryption: PKI +AES**
- **Device specific encryption keys, controlled by system owner**
- **Remote & local lockdown**
- **Over-the-air firmware upgrades**
- **Manual & programmable office mode**
- **Integrated door ajar and tamper sensor**
- **Remote unlock**
- **No software or lease licenses**

Mechanical specifications

Handing	Handed, field reversible; ADA compliant
Certifications/Compliance	Grade 1 ANSI/BHMA A156.13 Series 1000; Lock body conforms to FF-H-106 Type 86/87; UL10c-3hour
Door Thickness	1-3/4" standard
Backset	2-3/4"
Lock Case	Heavy gauge plated steel
Lever Design	Tango
Lever Functionality	Non-clutched
Strikes	Stainless steel, 4 7/8" X 1 1/4" curved lip ANSI strike
Keying	Hands-free U-Key™
Function	Passage, privacy, entry, classroom, storeroom; other functions available upon request
Outer Case	Satin stainless steel (630)
Dimensions	O/S 9-3/8" x 3-1/8" x 27/32"
Vandal Protection	Integrated tamper sensors
Door Ajar Alarm	Integrated deadlatch sensor
Mechanical Warranty	2 years

Mortise Door Reader SA-MDR

How it works



SA-MDR Options

Keying	In addition to U-Key™ operation: 10-key pushbutton; Proximity and Smartcard; Bluetooth
Lever Design	Quest, Sentinel
Lever Functionality	Clutched (free-wheeling)
Finish	Satin brass (606) Oil rubbed bronze (613) Satin nickel (619) Satin chrome (626)
Door Thickness	Contact factory for options
Outdoor Usage	Weatherized
Saniguard	Antimicrobial coating

Frequently asked questions

1. **Do locks come with access options other than a U-Key™?** This lock supports SecureALL U-Key™, Proximity and Smartcard credentials. Options are available to add a cost effective 10-button keypad and/or a mechanical (SFIC) key cylinder.
2. **Where does access control information reside in the system?** The SA *Guardian* automatically sends this information to each applicable lock. The lock is then fully capable of making access control decisions without going back to the Server. As locks are battery operated, doors will continue to function, even in the event of a power failure.
3. **What is tracking capability:** Each lock has the built-in ability to automatically track a hands-free U-Key™ (person or asset) as it passes by the door. It can optionally be turned on.
4. **How many lock units can be controlled by a single router?** There is no limit to the number of doors that can be controlled by a single router (limited only by building construction) and no licenses are required.
5. **Can a U-Key™ unlock a door when approached from inside?** SecureALL locks are designed to know whether a U-Key™ is located inside or outside a room. Therefore, a door can never unlock by accident when approached from inside, i.e. looking though a door peephole.
6. **Does the system send a low battery alarm?** When batteries in any of the system components reach a programmed minimum level, an individual designated by the system administrator is notified, via the client screen, email or text message, that batteries must be changed.
7. **What level of encryption is incorporated in the system?** SecureALL utilizes multiple levels of encryption (PKI and AES), first to ensure that any equipment being added to a customer's system is genuine, and then to guarantee that end-to-end communication between all layers is secure at the highest possible level. Customers have complete control over encryption keys.
8. **Can a door be unlocked if the batteries are dead?** An auxiliary power supply is available that energizes the door lock, allowing an authorized U-Key™ entrance to a room.
9. **Lock installation tools?** Ordinary workbench tools; no special programmer or cable.

SECUREALL SECURITY REINVENTED℠

Mortise Door Reader SA-MDR w/Card Option

Features & Benefits

- **Hands-free, multi-distance access**
- **Proximity and Smartcard**
- **Long range, hands-free asset tracking**
- **Real-time, extreme low power communication => long battery life**
- **All access decisions at the door; does not require server link**
- **Multi-layer hard encryption: PKI +AES**
- **Device specific encryption keys, controlled by system owner**
- **Remote & local lockdown**
- **Over-the-air firmware upgrades**
- **Manual & programmable office mode**
- **Integrated door ajar and tamper sensor**
- **Remote unlock**
- **No software or lease licenses**

Electrical specifications

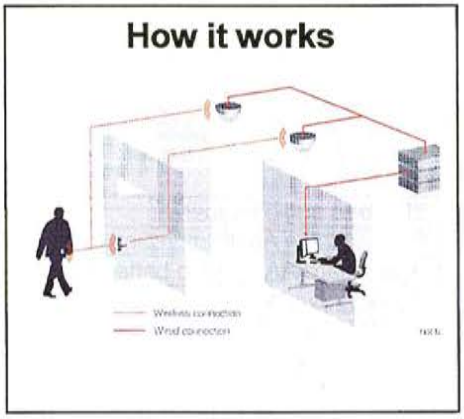
Users	Up to 70,000
Audit Trail	6 mos. data stored in server, typical
Credential Verification Time	< 50ms
Visual/Audible Interface	LED and audio beeper
System Interface	SA-*Guardian* Application Server
Power Supply	4 standard AA alkaline batteries
Battery Life	4 years, typical
Exterior Operating Temperature	-10° C to +70° C or +14° F to +158° F
Interior Operating Temperature	-10° C to +55° C or +14° F to +131° F
Certifications/Compliance	FCC Part 15 B&C
Reader Technology: Hands free U-Key™ : Contactless Smart card: Bluetooth/Smartphone:	 Hands-free, wireless, PKI, AES ISO 14443, sector cryptography Bluetooth (BLE)
Reader Frequency	2.4 GHz and 13.56 MHz
Reader Range	U-Key™ : 1" to 30 ft, programmable Card and BLE: 1"
Communication Security	PKI, AES-128
Encryption Keys	Device specific, customer controlled
Wireless Communication Protocol	Proprietary: Extreme low power (ELP) protocol & 802.15.4; 14443
Reader/Router Handshake	Automatic
Firmware Updates	PKI; over-the-air
Electrical Warranty	2 years

Mechanical specifications

Handing	Handed, field reversible; ADA compliant
Certifications/Compliance	Grade 1 ANSI/BHMA A156.13 Series 1000; Lock body conforms to FF-H-106 Type 86/87; UL10c-3hour
Door Thickness	1-3/4" standard
Backset	2-3/4"
Lock Case	Heavy gauge plated steel
Lever Design	Tango
Lever Functionality	Non-clutched
Strikes	Stainless steel, 4 7/8" X 1 1/4" curved lip ANSI strike
Keying	Hands-free U-Key™, Card, BLE
Function	Passage, privacy, entry, classroom, storeroom; other functions available upon request
Outer Case	Satin stainless steel (630)
Dimensions	O/S 9-3/8" x 3-1/8" x 27/32"
Vandal Protection	Integrated tamper sensors
Door Ajar Alarm	Integrated deadlatch sensor
Mechanical Warranty	2 years

Mortise Door Reader SA-MDR w/Card Option

How it works



SA-MDR Options

Keying	In addition to U-Key™ operation: 10-key pushbutton;
Lever Design	Quest, Sentinel
Lever Functionality	Clutched (free-wheeling)
Finish	Satin brass (606) Oil rubbed bronze (613) Satin nickel (619) Satin chrome (626)
Door Thickness	Contact factory for options
Outdoor Usage	Weatherized
Saniguard	Antimicrobial coating

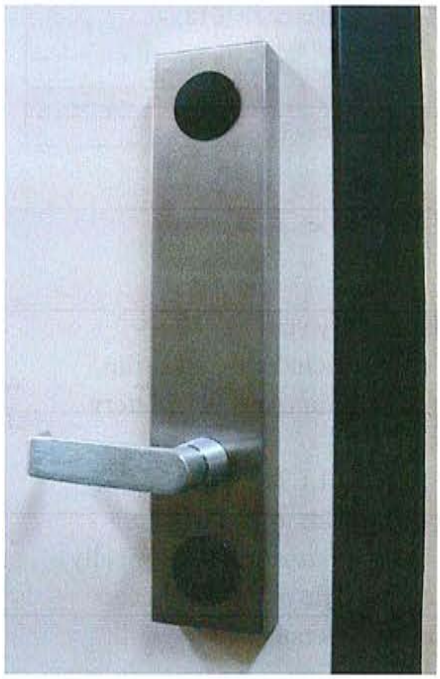
Frequently asked questions

1. **Do locks come with access options other than a U-Key™?** This lock supports SecureALL U-Key™, Proximity and Smartcard credentials. Options are available to add a cost effective 10-button keypad and/or a mechanical (SFIC) key cylinder.
2. **Where does access control information reside in the system?** The SA *Guardian* automatically sends this information to each applicable lock. The lock is then fully capable of making access control decisions without going back to the Server. As locks are battery operated, doors will continue to function, even in the event of a power failure.
3. **What is tracking capability:** Each lock has the built-in ability to automatically track a hands-free U-Key™ (person or asset) as it passes by the door. It can optionally be turned on.
4. **How many lock units can be controlled by a single router?** There is no limit to the number of doors that can be controlled by a single router (limited only by building construction) and no licenses are required.
5. **Can a U-Key™ unlock a door when approached from inside?** SecureALL locks are designed to know whether a U-Key™ is located inside or outside a room. Therefore, a door can never unlock by accident when approached from inside, i.e. looking though a door peephole.
6. **Does the system send a low battery alarm?** When batteries in any of the system components reach a programmed minimum level, an individual designated by the system administrator is notified, via the client screen, email or text message, that batteries must be changed.
7. **What level of encryption is incorporated in the system?** SecureALL utilizes multiple levels of encryption (PKI and AES), first to ensure that any equipment being added to a customer's system is genuine, and then to guarantee that end-to-end communication between all layers is secure at the highest possible level. Customers have complete control over encryption keys.
8. **Can a door be unlocked if the batteries are dead?** An auxiliary power supply is available that energizes the door lock, allowing an authorized U-Key™ entrance to a room.
9. **Lock installation tools?** Ordinary workbench tools; no special programmer or cable.

SECUREALL SECURITY REINVENTED℠

Panic Hardware Reader SA-PHR

(designed for new and retrofit installation into non-electrified Von Duprin 98/99 Series Rim hardware)



Features & Benefits

- **Hands-free, multi-distance access**
- **Long range, hands-free asset tracking**
- **Real-time, extreme low power communication => long battery life**
- **All access decisions at the door; does not require server link**
- **Multi-layer hard encryption: PKI +AES**
- **Device specific encryption keys, controlled by system owner**
- **Remote & local lockdown**
- **Over-the-air firmware upgrades**
- **Manual & programmable office mode**
- **Integrated door ajar and tamper sensor**
- **Remote unlock**
- **No software or lease licenses**

Electrical specifications

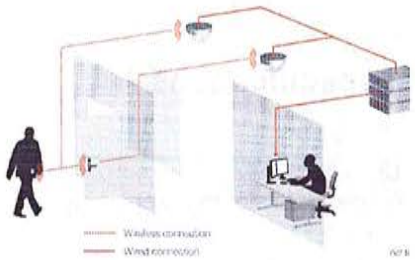
Users	Up to 70,000
Audit Trail	6 mos. data stored in server, typical
Credential Verification Time	< 50ms
Visual/Audible Interface	LED and audio beeper
System Interface	SA-*Guardian* Application Server
Power Supply	3 standard C alkaline batteries
Battery Life	8 years, typical
Exterior Operating Temperature	-10° C to +70° C or +14° F to +158° F
Interior Operating Temperature	-10° C to +55° C or +14° F to +131° F
Certifications/Compliance	FCC Part 15 B&C
Reader Technology	Hands-free, wireless
Reader Frequency	2.4 GHz
Reader Range	1" to 30 ft, programmable
Communication Security	PKI, AES-128
Encryption Keys	Device specific, customer controlled
Wireless Communication Protocol	Proprietary: Extreme low power (ELP) protocol & 802.15.4
Reader/Router Handshake	Automatic
Firmware Updates	PKI; over-the-air
Electrical Warranty	2 years

Mechanical specifications

Handing	Handed, field reversible; ADA compliant
Certifications/Compliance	UL10c-3hour
Door Thickness	1-3/4" to 2-1/4"
Backset	2-3/4"
Lever Design	Dane
Lever Functionality	Non-clutched
Keying	Hands-free U-Key™
Function	Passage, entry, classroom
Case Material	Satin stainless (630)
Dimensions	O/S 14-3/8" x 3-1/8" x 1-1/8"
Vandal Protection	Integrated tamper sensors
Door Ajar Alarm	Integrated deadlatch sensor
Mechanical Warranty	2 years

Panic Hardware Reader SA-PHR

How it works



SA-PHR Options

Keying	In addition to U-Key™ operation: 10-key pushbutton; Proximity and Smartcard; Bluetooth
Lever Design	Quantum
Finish	Satin brass (606) Oil rubbed bronze (613) Satin chrome (626)
Door Thickness	Contact factory for options
Outdoor Usage	Weatherized
Saniguard	Antimicrobial coating

Frequently asked questions

1. **What does the PHR kit comprise?** PHR is designed to convert an industry standard VDP-98/99 series exit device into a wireless, centrally controlled lock. The kit includes outside trim, inside trim-cover with built-in SecureALL electronics, latch bolt sensorization package, battery box and local lock-down button.
2. **Do locks come with access options other than a U-Key™?** All SecureALL locks can be equipped with a cost effective 10-button keypad. Prox and smartcard options also available.
3. **Where does access control information reside in the system?** The SA *Guardian* automatically sends this information to each applicable lock. The lock is then fully capable of making access control decisions without going back to the Server. As locks are battery operated, doors will continue to function, even in the event of a power failure.
4. **What is tracking capability:** Each lock has the built-in ability to automatically track a hands-free U-Key™ (person or asset) as it passes by the door. It can optionally be turned on.
5. **How many lock units can be controlled by a single router?** There is no limit to the number of doors that can be controlled by a single router (limited only by building construction) and no licenses are required.
6. **Can a U-Key™ unlock a door when approached from inside?** SecureALL locks are designed to know whether a U-Key™ is located inside or outside a room. Therefore, a door can never unlock by accident when approached from inside, i.e. looking though a door peephole.
7. **Does the system send a low battery alarm?** When batteries in any of the system components reach a programmed minimum level, an individual designated by the system administrator is notified, via the client screen, email or text message, that batteries must be changed.
8. **What level of encryption is incorporated in the system?** SecureALL utilizes multiple levels of encryption (PKI and AES), first to ensure that any equipment being added to a customer's system is genuine, and then to guarantee that end-to-end communication between all layers is secure at the highest possible level. Customers have complete control over encryption keys.
9. **Can a door be unlocked if the batteries are dead?** An auxiliary power supply is available that energizes the door lock, allowing an authorized U-Key™ entrance to a room.

SECUREALL SECURITY REINVENTED℠

Panic Wall Reader SA-PWR

(designed for new and retrofit installation with a panic exit door utilizing electric latch retraction)

Features & Benefits

- **Hands-free, multi-distance access**
- **Long range, hands-free asset tracking**
- **No cable required between PWR and I/O Adapter**
- **Real-time, extreme low power communication => long battery life**
- **All access decisions at the door; does not require server link**
- **Multi-layer hard encryption: PKI +AES**
- **Device specific encryption keys, controlled by system owner**
- **Remote & local lockdown**
- **Over-the-air firmware upgrades**
- **Manual & programmable office mode**
- **Remote unlock**
- **No software or lease licenses**

Electrical specifications - PWR

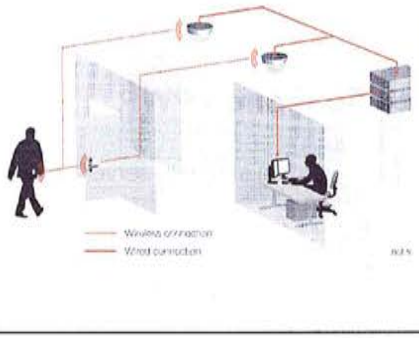
Users	Up to 70,000
Audit Trail	6 mos. data stored in server, typical
Credential Verification Time	< 50ms
Visual Interface	LED
System Interface	SA-*Guardian* Application Server
Power Supply	4 standard AA alkaline batteries; or 12-24VDC
Battery Life	4 years, typical
Exterior Operating Temperature	-10° C to +70° C or +14° F to +158° F
Interior Operating Temperature	-10° C to +55° C or +14° F to +131° F
Certifications/Compliance	FCC Part 15 B&C
Reader Technology	Hands-free, wireless
Reader Frequency	2.4 GHz
Reader Range	CAT 5 wired, 1000'; Wireless, 100'; programmable
Communication Security	PKI, AES-128
Encryption Keys	Device specific, customer controlled
Wireless Communication Protocol	Proprietary: Extreme low power (ELP) protocol & 802.15.4
Reader/Router Handshake	Automatic
Firmware Updates	PKI; over-the-air
Electrical Warranty	2 years

Mechanical specifications - PWR

Keying	Hands-free U-Key™; Proximity and Smartcard; Bluetooth
Function	Entry, classroom
Case Material	Satin stainless (630)
Dimensions	O/S 4-3/4" x 4-3/4" x 1-1/4"
RF Directional Control	0° ± 30° , programmable
Mounting Options	Double gang electrical box mounted directly to a flat wall; glass mounted on a window; mounted on a door frame
Vandal Protection	Integrated tamper sensors
Outdoor Usage	Weatherized; must use mechanical backing plate and caulking
Mechanical Warranty	2 years

Panic Wall Reader SA-PWR

How it works



Electrical Specifications - I/O Adapter

Power Supply	12-24 VDC, .1A
Operating Temperature	-10° C to +55° C or +14° F to +131° F
Input Ports	Quantity = 3; Dry contact; < 1000Ω
Output Ports	Quantity = 2; Dry contact; Max 24VDC, .1A

Mechanical Specifications - I/O Adapter

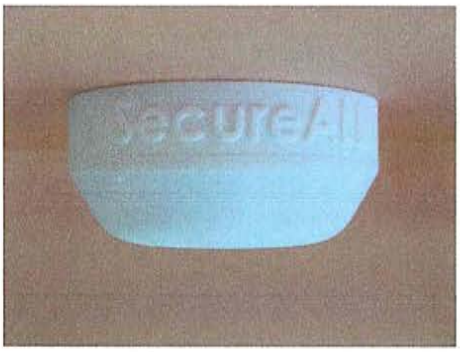
Case Material	Plastic
Dimensions	O/S 4-7/8" x 1-15/16" x 1"
Mounting Options	Inside electrical control box; wall mounted near electrical control box
Mechanical Warranty	2 years

Frequently asked questions

1. **What does the PWR kit comprise?** A PWR wirelessly controls a door that is typically used for building entrance and has an electric strike, a latch retractor or ADO (Automatic Door Operator). The kit is contains a PWR and an IO-Adapter. The IO-Adapter provides dry-contact output to the door electric controller. The PWR connects to the server via a wireless link to a nearby router.
2. **How are the PWR and I/O Adapter connected?** The PWR can be connected to the I/O Adapter with either a CAT5 cable or via wireless communication if running a cable is not feasible.
3. **How is the PWR reader directionality changed?** The RF beam can be configured, via a remote configuration command, to be broadside or steered +/- 30° to point in the direction of the desired user entry path.
4. **Where does access control information reside in the system?** The SA *Guardian* automatically sends this information to each applicable lock. The lock is then fully capable of making access control decisions without going back to the Server. As locks are battery operated, doors will continue to function, even in the event of a power failure.
5. **Can a U-Key™ unlock a door when approached from inside?** SecureALL locks are designed to know whether a U-Key™ is located inside or outside a room. Therefore, a door can never unlock by accident when approached from inside, i.e. looking though a door peephole.
6. **Does the system send a low battery alarm?** When batteries in any of the system components reach a programmed minimum level, an individual designated by the system administrator is notified, via the client screen, email or text message, that batteries must be changed.
7. **What level of encryption is incorporated in the system?** SecureALL utilizes multiple levels of encryption (PKI and AES), first to ensure that any equipment being added to a customer's system is genuine, and then to guarantee that end-to-end communication between all layers is secure at the highest possible level. Customers have complete control over encryption keys.
8. **Can a door be unlocked if the batteries are dead?** No. The batteries however can be changed on the PWR as it is mounted using security screws on exterior side of controlled space.

SECUREALL SECURITY REINVENTED℠

Router (Access Point) SA-ROU



Electrical specifications

Number of Doors Controlled	Unlimited, restricted only by distance to door reader and building construction
Visual Interface Verification	Flashing yellow and solid green LEDs
System Interface	SA-*Guardian* Application Server via a POE switch
Power Supply	POE or 5VDC
Backup Battery Life	8 hours; automatically recharges with trickle current
Operating Temperature	-10° C to +70° C or +14° F to +158° F
Certifications/Compliance	FCC Part 15 B&C
Communication Link	10 Base T, RJ45
Operating Frequency	2.4 GHz
Max Communication Range	1000'
Communication Security	PKI, AES-128
Encryption Keys	Device specific, customer controlled
Wireless Communication Protocol	Proprietary: Extreme low power (ELP) protocol & 802.15.4
Reader/Router Handshake	Automatic
Firmware Updates	PKI; both U-Key™ and door readers
Electrical Warranty	2 years

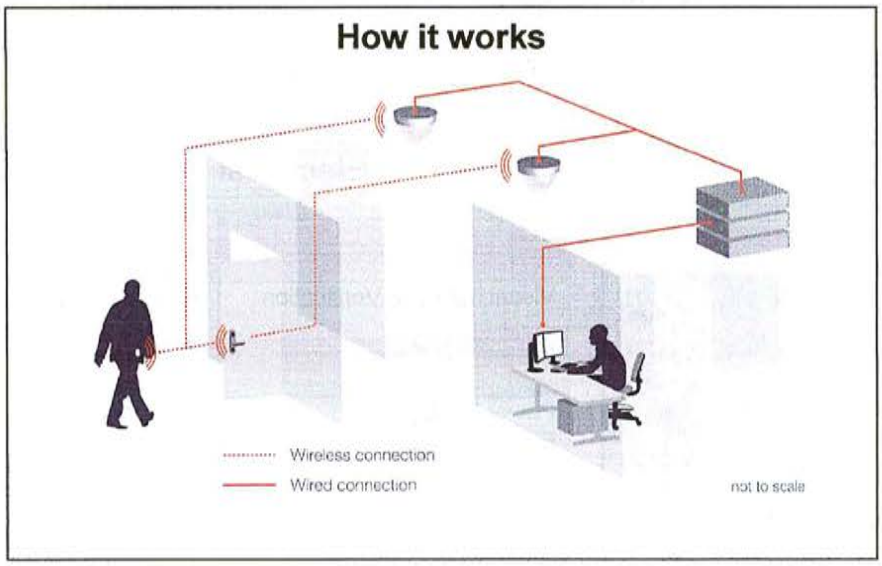
Features & Benefits

- **Utilizes static IP address or DHCP**
- **Power-Over-Ethernet or DC voltage**
- **Communicates with both door readers and U-Keys™**
- **Overlapping coverage of routers yields automatic failover in the event of an electrical problem**
- **Real-time, extreme low power communication**
- **Device specific encryption keys, controlled by system owner**
- **Over-the-air firmware upgrades**
- **Integrated tamper sensors**
- **No software or lease licenses required**

Mechanical specifications

Case Material	Plastic
Dimensions	O/S 4" diameter x 1-7/8"
Mounting Options	Ceiling level; above a drop ceiling; wall mounted. For custom mounting, consult with factory
Vandal Protection	Integrated tamper sensors
Outdoor Usage	Weatherized; must use mechanical backing plate and caulking
Mechanical Warranty	2 years

Router (Access Point) SA-ROU



Frequently asked questions

1. **How many lock units can be controlled by a single router?** There is no limit to the number of doors that can be controlled by a single router and no licenses are required.
2. **What is typical router range?** Even with SecureALL's patented Extreme Low Power (ELP) technology, in free space, communication range is approximately one-half mile. Within a building, this is limited only by construction materials and hallway shape.
3. **How is optimum router placement determined?** Certified installers will do a building site audit, utilizing SecureALL test equipment, to determine optimized router locations.
4. **What is "automatic failover?"** If desired, routers can be positioned within a building so every door has coverage from at least two routers (in some cases, this will be between floors). The router with the strongest communication link is always primary coverage for a particular door. In the event of a disconnection, the second router will automatically take over. No manual intervention is required.
5. **What type of alarm will be sent in the event of a router disconnect?** As with any problem occurring in the *Guardian* system, alarms are sent to the individual(s) having oversight for that particular part of the system, either through email, text, or sms.
6. **What is "auto-discovery" between routers and readers and how does this facilitate installation?** Access control lists (ACLs) are stored in the *Guardian* server. Upon installation of a router and door lock, the ACL is transmitted first to the router and then automatically sent to the door lock. The same process is used for ACL changes and firmware updates. There is never a need for any handheld device to program door locks, saving significant employee time.
7. **What type of communication device addresses are available?** Depending on preference, routers can be programmed for static IP addresses or DHCP.
8. **How does SecureALL prevent spoofing of any hardware by a third party?** PKI encryption is used to ensure that any equipment being added to a customer's system is genuine. Unless the correct handshake occurs, the *Guardian* system will reject that component as not valid.

SECUREALL SECURITY REINVENTED℠

Tracker SA-TRK

Electrical specifications

Number of tracked U-Keys or Tags	Unlimited
Credential enumeration rate	Up to 100 credentials per second
System Interface	Guardian software
Power Supply	5V DC or PoE
Backup Battery Life	8 hours; automatically recharges with trickle current
Visual Interface Verification	Flashing yellow and solid green LEDs
Operating Temperature	0° C to +70° C
Certifications/Compliance	FCC Part 15 B&C
Reader Technology	Hands-free, wireless
Reader Frequency	2.4 GHz
Reader Range	1" to 100 ft, programmable
Communication Security	PKI, AES
Wireless Communication Protocol	Proprietary: Extreme low power (ELP) protocol & 802.15.4
Electrical Warranty	2 years

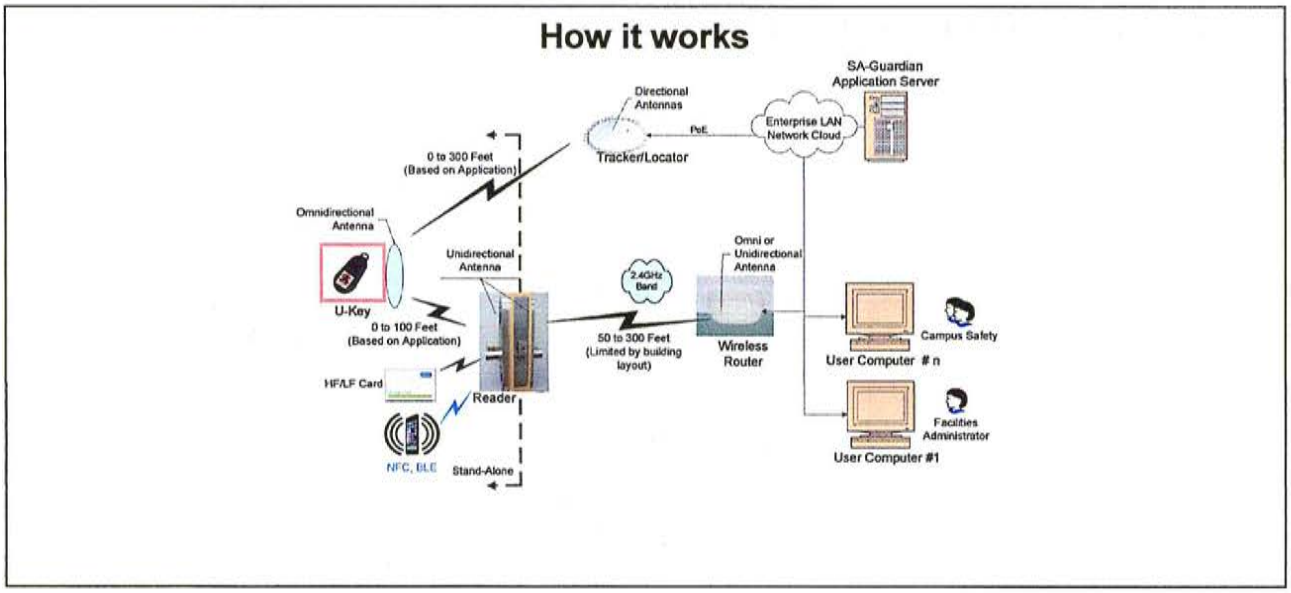
Features & Benefits

- **Enumerates an unlimited number of U-Key™ or Tag credentials.**
- **Reports approximate location of enumerated credentials.**
- **Can be configured for two modes of operation:**
  - **On-demand: Tracker is normally inactive and only scans for credentials when required, i.e. to determine locations of people in emergencies.**
  - **Continuous: Tracker continuously monitors credentials in its vicinity, i.e. to verify presence of asset tags.**
- **Connection to the Guardian system is either wireless (through an SA-ROU device) or wired over Ethernet.**
- **Utilizes static IP address or DHCP**
- **Power-Over-Ethernet or DC voltage**

Mechanical specifications

Case Material	Plastic
Dimensions	5" diameter X 2" high
Mounting Options	Ceiling level; above a drop ceiling; wall mounted. For custom mounting, consult with factory
Vandal Protection	Integrated tamper sensors
Mechanical Warranty	2 years

Tracker SA-TRK



Frequently asked questions

1. **How does the Tracker determine the location of U-Keys™ or U-Tags?** The tracker has many directional antennas, each pointing in a different direction. When communicating with U-Keys™ or U-Tags, the tracker analyses the received RF signal strength on each of the antennas to get an indication of the direction of the credential. The received signal strength gives an indication of distance. When the same credential is in range of multiple trackers, server software can refine location accuracy by combining this information.
2. **How does the Tracker communicate with the SA-Guardian server?** The Tracker has an Ethernet port and can be connected directly to a local area network. If this is not practical, the Tracker can also communicate wirelessly, as long as it is installed within the range of one or more SecureALL routers.
3. **How often does the Tracker perform a scan and update the location of credentials?** This is configurable and can be as often as every five seconds.
4. **What level of encryption is incorporated in the system?** SecureALL utilizes multiple level of encryption (PKI and AES), first to ensure that any equipment being added to a customer's system is genuine, and then to guarantee that end-to-end communication between all layers is secure at the highest possible level. Customers have complete control over encryption keys.

Addendum #6 8/1/17

SecureALL Feature List

SECUREALL SECURITY REINVENTED℠ June 13, 2017

SecureALL Feature List

1. No yearly-use Access Control System licensing fees of any kind.
2. Full turnkey, total security solution:
    a) Not just simple access control but optionally: asset and personnel tracking, non-motion detection, activity management (time and attendance), disaster evacuation control and monitoring, emergency-call/distress signaling, point-of-sale, and zero-barrier tailgate detection.
    b) Lowest "Total Cost of Ownership," including potential insurance savings.
    c) Single vendor for fast support and accountability.
3. Patented Extreme Low Power (ELP) technology enables real-time communication (no duty-cycling), yielding the equivalent of wired security but with wireless cost. Also allows the full integration of features shown in 2a above.
    a) High speed, license-free wireless system, operates in the 2.4 GHz band from credential to lock and 802.15.4 from lock to router (no control panel).
    b) Green Technology: Lock units run on 3 or 4 standard AA alkaline batteries, with extreme long battery life, 4 - 7 years.
    c) High performance, energy optimized lock actuator typically outperforms the competition by 2-4 times in the number of door openings per battery change.
4. Complete product suite: Server + integrated control software; Routers (Access Points); Repeaters; Trackers; Cylindrical Locks; Mortise Locks; Wireless or Wired Wall Readers for electrified panic exit devices (including gate and garage openers); Retrofit Kits for non-electrified panic exit devices; Privacy Locks; Passage Locks. Weatherized version of each is available.
    a) Multiple credentials available for access control. Credential verification time < 50ms after completion of communication sequence:
        i. U-Key™ - Variable distance (1" to 75'), hands-free technology. Highest cryptographic protection.
        ii. Card - 13.56 MHz contactless HID iClass SE & SEOS (best cryptography among cards).
        iii. Card - 125 KHz proximity.
        iv. PKI based, highly secure Bluetooth Low Energy (BLE) phone credential.
        v. 10 key pushbutton, remotely reconfigurable codes.
        vi. SFIC hard key lock.
    b) Locks are ANSI Grade 1; UL 10c-3 hour.
    c) Access control software can run on a Windows or Linux based server. Can be dedicated hardware or VM. Server is capable of managing up to 100K doors.
    d) Routers are Powered Over Ethernet (PoE). Repeaters can be AC powered or 5VDC.
        i. Routers control an unlimited number of locks. Communication range is 1/2 mile in free space. Building construction can limit router coverage.
    e) Cylindrical and mortise locks come equipped with integrated latch sensors and door ajar/position sensors, eliminating extra cost at installation.
    f) Panic wall readers utilize a wireless link to a SecureALL I/O Adapter that creates a "dry contact closure" to trigger an electric strike plate or automatic door operator. The wall reader has a $\pm 30^{\circ}$ steerable beam to optimize coverage of hands-free U-Key™ entry.
    g) All lock/unlock decisions are made at the door, not at the server. Locks are battery operated, ensuring locks continue to work during a power failure or network outage.

h) Up to 12,500 events are stored in each lock while offline. When online, data are uploaded to the server and then archived for history.
i) User capacity per door = 70,000.
j) Locks come equipped with both visual (LED) and audible (beeper) entry validation.

5. Encryption: No single point of encryption exposure. Each device has its own unique encryption key.
   a) Encryption keys are managed by the system administrator. AES keys are electronically distributed using PKI cryptography infrastructure.
   b) Encryption keys can be changed any time, manually or automatically.
   c) Encryption includes end-to-end PKI based session AES and two link level AES security.
   d) Secure "circle of trust" guarantees only genuine SecureALL equipment is installed. Cannot be hacked or spoofed.
      i. Legitimate devices are automatically imported via a manifest file.
      ii. When a device is powered, it performs a mutual authentication via hard cryptographic protocol before pairing up.
      iii. Automatic discovery and connection occurs as devices are brought on line.
6. All device programming (locks and U-Keys™) is "over-the-air" from a single server with unique endpoint-to-endpoint encryption. Communication integrity is ensured by PKI based authentication and secure AES key exchange.
   a) Devices are capable of checking that new firmware has been properly downloaded. If not, previous version is restored.
   b) No hand-held computer is required to manually program or re-configure locks or to distribute AES encryption keys. This yields a significant savings in ownership cost. It also eliminates exposure from having encryption keys resident in a portable device.
7. Plug and play installation:
   a) Locks automatically discover the best available router within wireless range.
   b) When a door is opened and the lock's spatial orientation changes, the best antenna for router communication is chosen, always ensuring a reliable and long range router wireless link.
   c) The lock continually evaluates alternative router connections and switches to the optimal wireless link.
   d) A door automatically discovers opening direction to initiate latch sensor configuration.
8. SecureALL locks are equipped with the most comprehensive lockdown solutions:
   a) Full campus, or any part of a campus, programmable via central server, within 10 seconds.
   b) Local (manual) lockdown at a door, available with instantaneous execution.
   c) Lockdown can be configured to allow access only to first responders.
      i. Four additional progressively graded lockdown entry levels available.
   d) Smart (reflex) lockdown: When multiple local lockdowns are initiated within a predefined period of time, an entire building can be configured to go into lockdown.
9. Easy to learn programming: Reusable constructs significantly reduce the effort required to setup and run the SA-Guardian.
   a) Administrator can easily assign credential users to "Access Groups" (that further comprise room schedules).
      i. Permanent rooms
         1. Access schedule is automatically generated and maintained.
         2. Validity granularity of "Start date & time" and "End date & time."
      ii. Permits exclusive or overlapping access to rooms well in advance of cut-over date (no need for last minute downloading of access information to the door lock).
      iii. No limit to the number of access groups that can be assigned to a credential user.
   b) Distributed system administration (patent pending)
      i. Fine grained privileges (roles) allow end user customization, such that many system administrators can exist, albeit with user specific privileges.

1. Ability to compartmentalize administrator's privileges to give access only to their designated "Access Domain".
2. Allows virtual partitioning of the campus for access, so that administrators are given delegated privileges only for their assigned buildings or set of rooms.
3. Alarm notification is scoped by administrator's "Alarm Domain."

c) Lock configuration parameters: Locks have a rich set of operating modes and configuration parameters that can be remotely viewed and modified via a secure encrypted connection. Each lock is uniquely configurable for at least the following operating parameters:
   i. Manual office mode - enable/disable
   ii. Manual office mode maximum period
   iii. Manual office mode forced expiration by time
   iv. Scheduled office mode : 'first card in' to start office mode– enable/disable
   v. Manual lockdown – enable/disable
   vi. Manual lockdown priority
   vii. Minimum user priority to activate local lockdown
   viii. Minimum user priority to cancel local lockdown
   ix. Door secure delay
   x. Door ajar time threshold
   xi. Door ajar local beeper - lead-in warning period
   xii. Door ajar period when device is in lockdown
   xiii. Low battery notification threshold
   xiv. Battery exhaustion notification threshold
   xv. Failsafe in locked state- threshold
   xvi. Failsafe in unlocked state - threshold
   xvii. U-Key™ activation standard distance
   xviii. U-Key™ activation distance when door is ajar
   xix. Current daylight savings time offset
   xx. Future daylight savings time offset
   xxi. Future date when next daylight saving time will be applied
   xxii. Antennas to be used to connect to best available router
   xxiii. Operating parameter of Extreme Low Power communication system
   xxiv. Logging verbosity level
   xxv. Maximum log level that triggers automatic transfer of logs to server
   xxvi. Maximum age of the log buffer that will result in sending logs to server
   xxvii. Pushbutton codes for locks with keypad

d) Lock status variables: Lock operating status can be remotely viewed via a secure encrypted connection:
   i. Door latch state
   ii. Lock state
      1. Office mode state
      2. Lockdown state
      3. Remote unlock state
   iii. Battery voltage
   iv. Quiescent operation load current
   v. Radio communication packet and message odometer: Good Rx count | Rx CRC error count | Rx timeout count | Good Tx count | Network scan count |
   vi. Visible network count
   vii. Actuator drive count
   viii. Router connection signal strength
   ix. Primary router
      1. Device-ID

2. Link budget
3. Network channel
4. Network cost

x. Secondary router
   1. Device-ID
   2. Link budget
   3. Network channel
   4. Network cost

xi. Firmware version

e) Lock events: Autonomously operating locks generate events to notify server in real-time of significant operating condition changes. Events can generate alarms depending on user need. List of available events:
   i. Tamper alert
   ii. Tamper alert normal
   iii. Low battery
   iv. Exhausted battery
   v. Lock actuator trouble
   vi. Door ajar
   vii. Manual lockdown engage
   viii. Manual lockdown end
   ix. Lockdown door ajar
   x. Sensor error
   xi. PWR & IO-adapter connected
   xii. PWR & IO-adapter disconnected
   xiii. PWR & IO-adapter paired
   xiv. Power supply change

f) Easily generated reports.

10. Simple segue to a cloud based SaaS model, for addressing small and medium sized businesses.