

# Strong Authentication Solution Request for Information (RFI)

---

[NOTE: SPECIFICS IN THIS RFI HAVE BEEN MODIFIED SO IT CAN BE USED AS A SAMPLE.]

## Contents

<b>CONTENTS</b> .....	<b>1</b>
<b>BACKGROUND</b> .....	<b>1</b>
OBJECTIVE.....	1
ABOUT THE DISTRICT .....	2
<b>REQUIREMENTS OF THE SOLUTION</b> .....	<b>2</b>
<b>RFI PROCESS</b> .....	<b>3</b>
PARTICIPATION IN THE RFI.....	3
EUSD INTENT .....	3
REQUESTED FORMAT FOR RESPONSES .....	4
TIMELINE OF EVENTS .....	4
QUESTIONS & CLARIFICATIONS.....	4
<b>RESPONSE INSTRUCTIONS</b> .....	<b>5</b>
LITERATURE REQUEST.....	5
PROPOSED SOLUTIONS.....	5
COSTS FOR PROPOSED SOLUTIONS .....	6
<b>CONTACT INFORMATION</b> .....	<b>6</b>

## Background

### OBJECTIVE

Example Unified School District (EUSD or “the District”) recently replaced its student information system (SIS), and now seeks to leverage this investment to provide enhanced functionality to teachers, students and parents. An immediate goal is to allow teachers to work with the SIS (and other applications) remotely (i.e., to review student work and record grades while at home).

The District IT staff supports this goal and has implemented a VPN infrastructure to achieve it. However, the IT staff has also identified an important security concern which must be resolved prior to offering remote access services to the teachers.

The concern stems from the District’s exceptionally high requirement for integrity of the SIS. This requirement is best expressed by example: it is a principal requirement of the District that student transcripts accurately reflect student performance; should the integrity of the SIS be compromised, then – regardless of the scope of the compromise - the validity of all student transcripts become questionable and this can have a harmful effect on the students and community. Obviously, this is an unacceptable outcome for the District.

Offering remote access to applications increases the risk of impersonation. Extending our example above, this would be someone successfully pretending to be a teacher or administrator (who has the ability to change grades and attendance records). This increased risk, in turn, increases the likelihood of an integrity compromise to the SIS.

The District’s current authentication practice is to require a user identifier and password to use applications. The District IT staff believes this (single-factor) practice is adequate for on-site use,

# Strong Authentication Solution Request for Information (RFI)

---

but likely inadequate for remote use. The gap is due to a person's ability to be physically onsite and using an authorized terminal contributing to the authentication process; when remote access is offered, this contribution is lost.

Therefore, the District is looking to enhance its authentication practice for remote access. To achieve this, the District would like to acquire an authentication solution for remote access that provides multi-factor (strong) authentication.

## ABOUT THE DISTRICT

EUSD is an 18,250 student, 17 site school district in Example County, California.

As of September, 2009, the District has the following staff that will desire remote access to the SIS (and other applications):

- 788 classroom teachers and counselors
- 40 administrators
- 15 psychologists
- 44 support staff

[NOTE: THIS SECTION REDACTED DUE TO PRIVACY CONCERNS – IT DISCUSSES THE DISTRICT'S TECHNICAL AND SECURITY ARCHITECTURE]

The District has standardized on Apple and HP personal computer hardware. Many staff have HP laptops. However, many staff do not have laptops or otherwise prefer to use a personal desktop PC when working from home. Personal PCs (at homes) comprise every imaginable combination of equipment vendors, operating systems, application software, etc. – and may be as much as 10 years old. The District does not currently, and does not wish to, provide support to staff in regards to their personal PCs.

The District IT staff includes qualified network, desktop, services, and security staff to support this initiative.

## Requirements of the Solution

We have identified the following, high level requirements for a multi-factor authentication solution:

1. As a non-profit, K12 educational organization, the District needs to procure a solution that achieves requirements at the lowest possible purchase cost and total cost of ownership.
2. The solution must achieve true multi-factor authentication; in addition to something the user knows (user ID / password / PIN), the solution must incorporate another factor such as something the user has (that cannot be reasonably replicated) or something the user is.
3. The solution must be easy for the staff to use.
4. The solution must be easy to support.
5. The solution must be easy to administer.
6. The amount of support required must be modest. The District lacks the staffing or resources for support-intensive solutions.
7. The solution must be readily integrated with Microsoft Active Directory and Cisco ASA VPN services.

# Strong Authentication Solution Request for Information (RFI)

---

8. The solution should work when teachers use any device capable of achieving the minimum environment required for our applications. The minimum environment includes Internet connectivity, and use of a web browser that supports SSL and ASP. Generally, if the teacher could use the application without the multi-factor solution installed, then it should work with it installed.
9. Solutions that do not require installation of software on end user devices are preferred. This is because the District wishes to avoid any circumstance where it is responsible for support for individually owned or offsite equipment.
10. To the extent that solutions have parts that can be lost or damaged by end-users (which is not desirable), the solutions should have expedited support processes for managing these parts (i.e., for replacement, revocation repair, etc.).
11. Such parts should have a high mean time to failure (i.e., years, not months).
12. The solution must provide real-time alerts when there are authentication failures or potential attacks.
13. The solution must provide an audit trail of successful and failed authentications.
14. The solution must incorporate strategies that discourage impersonation (i.e., lockouts, timeouts, etc.)
15. The solution should offer configurations that offer redundancy and high availability.
16. The solution should scale from 880 participants to 45,000 (in the event the District extends this security architecture to students and parents).

## RFI Process

### PARTICIPATION IN THE RFI

EUSD has invited 8-12 vendors to respond to this RFI. Initial vendor selection was based on a combination of reputation, research, and membership in OATH.

### EUSD INTENT

EUSD has prepared this RFI to learn about multi-factor authentication solutions from leading vendors. We expect to use the results of this RFI to:

- Understand the “state of the art”
- Select one or more appropriate architectures
- Refine our requirements
- Guide our selection process

Our selection process is unclear at this juncture; it will be defined by the:

- Nature of the solutions
- Total cost, and the timing of costs
- How offerings are differentiated
- Financial and market position of vendors
- The District’s compliance and process requirements

# Strong Authentication Solution Request for Information (RFI)

---

The District may be able to (and choose to) select a vendor based on the RFI responses. Alternately, the District may be required to (or may choose to) issue an RFQ/RFP.

## REQUESTED FORMAT FOR RESPONSES

This RFI requests:

1. Relevant product literature
2. One or more proposed solutions
3. Costs for the proposed solution(s)

We would be pleased to receive your response electronically (i.e., email, ftp, CD) in a variety of formats (i.e., PDF, HTML, Word, Excel). We will also accept hardcopy through a mail service. If you use a mail service, please make sure delivery occurs before responses are due.

**We need to receive all responses by 4:00 PM on November 20th.** Please do not feel constrained to provide everything at once; we are happy to receive your response in sections.

## TIMELINE OF EVENTS

Date	Time (PST)	Event
10/25/09	N/A	RFI is sent to selected vendors
10/26/09	7:00AM	EUSD will start to accept questions and requests for clarifications via electronic mail.
11/09/09	5:00PM	Last opportunity to submit questions and requests for clarifications.
11/14/09	4:00PM	All answers to submitted questions have been sent.
11/20/09	4:00 PM	RFI responses are due; late responses may not be considered.

## QUESTIONS & CLARIFICATIONS

Should you have any questions or need clarification, please email Mr. Creighton Grenoble at [cgrenoble@eusd.k12.ca.us](mailto:cgrenoble@eusd.k12.ca.us). Mr. Grenoble will reply to everyone receiving this RFI. EUSD will not respond to questions asked via telephone or in person.

All questions and requests for clarifications must be submitted by the date and time specified in the Timeline of Events; answers will be sent according to this timeline as well. Questions submitted after this deadline will not be answered.

Please do not contact EUSD personnel directly regarding this RFI. Vendors who contact any member of the board of education, administrators or staff without following the above listed protocol will be eliminated from further consideration.

Oral communications of EUSD employees, contractors and consultants concerning this RFI shall not be binding on EUSD.

# Strong Authentication Solution Request for Information (RFI)

---

## Response Instructions

### LITERATURE REQUEST

Please select and forward to us targeted and relevant sales material, white papers, case studies, technical documentation, etc. that will help us understand:

- The architecture and components of the system
- Functionality and features
- System administration processes
- Monitoring and auditing
- End-user training and support requirements and processes
- Cost; the timing of costs; total cost of ownership
- Company success and vision
- Features, algorithms, etc. that differentiate you from your competitors
- The support and maintenance processes

### PROPOSED SOLUTIONS

Please review our requirements and District overview above. After consideration, if you feel your company offers one or more attractive solutions, then please propose them to us.

Please do not feel constrained to offering us a single solution. If you have multiple solutions that meet our requirements, please provide us with some excellent alternatives.

For each solution you propose, please include the following:

- Diagrams and pictures that: show the solution as a whole; amplify how key components work together; and highlight how the “backend” integrates with our (or typical) network and services infrastructures.
- A write-up (document and/or presentation formats are fine) of the solution that explains the components, processes, etc.
- Specifications and requirements of the various components that make up your solution.
- A detailed walkthrough of the authentication process. This should include the perspective of the end-user, the VPN service, Active Directory and a web based application (which is Active Directory integrated). Please also include details as to what happens when authentication is successful and unsuccessful.
- A discussion of what we can expect from a system administration and help desk perspective.
- Your opinion as to the differentiating benefits of your solution; if you propose more than one alternative, we would appreciate your input as to the comparative pros and cons of your alternatives (i.e., why might we select one alternative over another).
- A confirmation that the solution meets all of our requirements (listed above), or a discussion of where there may be concerns that merit further discussion.
- An itemization of all the components required to fully implement the solution.
- Information (if any) about web links or demonstration environments which might improve our understanding of your proposal.

# Strong Authentication Solution Request for Information (RFI)

---

You may include more information in your proposal; please be sure to include the items above as a minimum.

## **COSTS FOR PROPOSED SOLUTIONS**

As a public entity with compliance requirements and a limited budget, the District is constrained in procuring a solution. A complex set of factors will determine whether the District can (or should) make a procurement decision from the RFI responses.

**Cost is a major factor for our selection. Key elements of cost, which we must understand to proceed, include:**

- Purchase cost (i.e., what must we pay to initially implement the solution).
- Recurring Cost (i.e., what we must pay annually for support, or what we should budget in future years for replacements).
- Five year cost of ownership (i.e., our total expected cash outlay for the first five years).
- The nature and purpose of each element of cost (because certain types of equipment, software and services are eligible for matching funds or grants; others are not).

Please provide us a cost analysis for each solution you propose. This analysis needs to clearly identify the four elements of cost shown above.

Please be as detailed and clear as possible; procurement is a complex process for a school district, and your clarity and completeness in identifying costs will be appreciated.

Also, we would be interested in learning your perspective on why your solution would offer the District with a low total cost of ownership (TCO) when compared to other vendor's offerings.

In evaluating responses to the RFI, the District plans to consider the cost analyses as accurate and representative. We will use them to compare solutions and as a basis for elimination; we may select a vendor based on the RFI responses. **Accordingly, please provide your best pricing in your RFI response rather than waiting for a RFP or RFQ.**

## **Contact Information**

If you have any questions or would like clarifications, please contact:

Creighton Grenoble  
Project Manager, EUSD  
Principal, Ascendant Services, Inc.

[Creighton@ascendantservices.com](mailto:Creighton@ascendantservices.com)

Example Unified School District  
123 Main Street  
Exampleville, CA 91234