



DataShield



The Security Division of EMC

DataShield RSA DLP Resident Services

Service Objectives

- To provide a design for a new RSA SecurID infrastructure including the planning of Authentication Manager, token provisioning, and token deployment.
- To cover our major service objectives with SecurID including Credential Management, Authentication, Contextual Authorization, and Intelligence.
- To provide the planning for protection with the 3 (three) Risk Management Factors which include security, convenience, and cost.

Scope of Work

- **Architecture:** Review the current policies of Credential Management including identity verification, identity and credential policy, and lifecycle management. Review the current policies of Authentication including the range of authentication mechanisms, the form factors of the solution, and the delivery platforms. Review the current policies of Contextual Authorization including access control, step-up authorization, and federation. Finally, we will review the Intelligence including identity and activity verification, proactive threat protection, and real-time information sharing.
- **Documentation:** produce an “as-is” access drawing, including credential management, authentication, contextual authorization, and intelligence.
- **Implementation:** Implementation of the SecurID appliance hardware, the SecurID authenticators (hardware, software, and SMS) and the SecurID agent software and the ongoing administration of the SecurID environment.
- **Work Hours:** Monday through Friday, normal work day 9:00 am EST to 6:00 pm EST. Weekend or after hours work will be billed on a Time and Material Basis at \$240 per hour.

Results and Customer Deliverables

- Verify and document all information risk management issues including credential management, authentication, contextual authorization, and intelligence for the customer.
- Verify and document the identification verification, the identity and credential policy, and the lifecycle management.
- Verify and document the range of authentication mechanisms, the choice of the form factors for the solution, and the delivery platforms.
- Verify and document the access control, the step-up authorization, and federation.
- Verify and document the identity and activity verification, the proactive threat protection, and the real-time information sharing

Acceptance Criteria

- A valid documentation set of the entire SecurID environment.
- Customer sign-off on agreed upon test plan each month.
- Knowledge transfer regarding the current state of your SecurID environment and plans for future security access.

Customer Prerequisites

- Provide administrator access to all hardware, software, tokens, and policies.
- Provide current operational requirements and policies of access.
- Provide sufficient operational requirements for completion of residency along with a secured working environment.

Pricing

- \$xx,xxx per month plus any associated travel expenses.

Contact Information: DataShield Consulting, LLC
Phone: (678) 232-4776