



Alternative Credentials for SIPRNet
Disadvantaged Users – Concept of Operations
(CONOPS)

DEFENSE INFORMATION SYSTEMS AGENCY

COMMON USER SERVICES

VERSION 1.0 – DRAFT 1

JANUARY 2013

Revision History

VERSION	PRIMARY AUTHOR(S)	DESCRIPTION OF VERSION	DATE COMPLETED
1.00	DISA	Initial Draft	01/29/2013

Disclaimer

The contents of this document are not to be construed as an official Defense Information Systems Agency document unless so designated by other authorized documents. The use of trade names in this document does not constitute an official endorsement or approval of the use of such commercial hardware or software. Do not cite this document for the purpose of advertisement.

Changes

Refer requests for all changes that affect this document to: CSD Operations Service Support Group

Disposition Instructions

Destroy this document when no longer needed. Do not return it to the organization. Safeguard and destroy this document with consideration given to its classification or distribution statement requirements.

Contents

Revision History	2
Disclaimer.....	3
Changes	3
Disposition Instructions	3
Introduction	5
Document Overview	5
Referenced Documents.....	5
Service Description	6
Objectives.....	6
Assumptions.....	6
Roles and Responsibilities.....	6
Business Processes.....	8
Functional Support to Users	8
ID Verification	9
Provisioning Trusted Agents	9
Internal Operations.....	9
Continuous Service Improvement	10
Bugs and Issues	10
Appendix A - Acronyms.....	11

Introduction

DISA Enterprise Services has received a request to build a solution that will allow an Enterprise User to authenticate to Enterprise Services using a temporary alternative Username and Password authentication mechanism while their Secret Internet Protocol Router Network (SIPRNet) Hard Token is being replaced. The delivered solution includes a web-based application and a set of processes that must be followed to allow a trusted agent to request temporary authentication credentials for Enterprise User.

This document outlines the internal operations and business processes necessary to support the Username and Password authentication solution for disadvantaged users on SIPRNet. It identifies the underlying assumptions behind operations, describes roles and responsibilities, and outlines the processes involved in supporting temporary Username and Password authentication into Enterprise Services.

Document Overview

The following describes how the document is laid out:

Introduction – This Section introduces the reader to the Username and Password solution and identifies other documents for reference.

Service Description – This describes the fundamental objectives and assumptions underlying the Username and Password solution. It also describes the Roles and Responsibilities for all parties involved.

Business Processes - This section identifies a full set of business processes in place to support operations. Many of the processes reference other documents that contain greater detail.

Appendices – The appendices are included listing reference information including an acronym list and error codes.

Referenced Documents

The following documents are referenced for this CONOPS:

- Solution Design - Enterprise Temporary Alternative Credentials
- Managers Guide to DEPO
- IdSS/EASF Configuration Management Plan
- IdSS/EASF Disaster Recovery Plan

Service Description

Here we outline the objects and assumptions underlying Username and Password operations.

Objectives

The following objectives form the foundation of Username and Password authentication solution design:

- Provide a way for a disadvantaged user to temporarily authenticate into DISA Enterprise Applications and Services without a SIPRNet token
 - When referring to disadvantaged user entails a user who has lost or damaged the user's SIPRNet Token and is in the process of obtaining a replacement
- Allow DISA mission partner to designate a responsible party to request soft credentials on behalf of the disadvantaged Enterprise User
- Maintain SIPRNetwork security posture

Assumptions

- DISA will deliver a username/password authentication solution by 2QFY13
- DISA Mission Partner will be responsible for validating whether an Enterprise user should be allowed a temporary username and password
- Enterprise Users must go through a designated Trusted Agent, a representative in the Mission Partner organization who is responsible for issuing a SIPRNet token to the user, to obtain a temporary username and password
- The Trusted Agent must authenticate with a SIPRNet Hard Token before a username and password can be generated
- The system must be able to support username and password access to Defense Enterprise Email (DEE) for up to 14 days to allow time for a disadvantaged user to receive a replacement SIPRNet Token
- The temporary passcode generated for password creation will be issued to the Trusted Agent, and the enterprise user must change password on first login
- The system clears the smartcard logon requirement from DEE after the user has provided the temporary passcode and reset their password
- The Username rather than the "Display Name" will be used by the system to identify the user.
- The temporary username and password will not be used for domain authentication

Roles and Responsibilities

- **Enterprise User** - The Enterprise User is the end user who must authenticate in order to access Enterprise Services. A 'disadvantaged' user is an Enterprise User temporarily lacking access to a SIPRNet Token but must access Enterprise Services while awaiting a token to be processed. The User is responsible for reaching out to the appropriate Trusted Agent to request a temporary username and password. After receiving the username and password, the Enterprise User is responsible for treating the username and password as SECRET information.
- **Trusted Agent** - The Trusted Agent is the agent within the Mission Partner organization who interacts with the Enterprise User and uses the solution to obtain the temporary username and password. The Trusted Agent is responsible for knowing how to access and use the tool, and making sure the agent has access to the solution during working hours. The Agent is also responsible validating that the Enterprise User should be allowed temporary username and password.
- **Group Managers** – Group Managers are responsible for identifying Trusted Agents for inclusion in the Trusted Advisor security group.

- **IdSS/EASF Product Manager** – The IdSS/EASF Product Manager manages and coordinates overall product development, maintenance, and operations behind the Username and Password authentication solution. The Product Manager makes all final decisions for development.
- **IdSS/EASF Configuration Manager** – The IdSS/EASF Configuration Manager coordinates the review, implementation, and versioning of changes to the Username and Password solution. All proposed updates to the deployed Username and Password solution must be submitted to the Configuration Manager formal Enhancement Requests.
- **DEE Service Desk** – The Help Desk will be available to handle technical issues.

Business Processes

The following business processes support operations underlying Username and Password Authentication for Disadvantaged Enterprise Users.

Functional Support to Users

'Disadvantaged' Users refer to Enterprise Users for SIPRNet but temporarily without access to a SIPRNet Token. These Users may have misplaced or damaged their token.

The process for an Enterprise User begins when the User requests a Trusted Agent to generate a reset passcode. Once the system generates the passcode the User enters the passcode into the system to create a password.

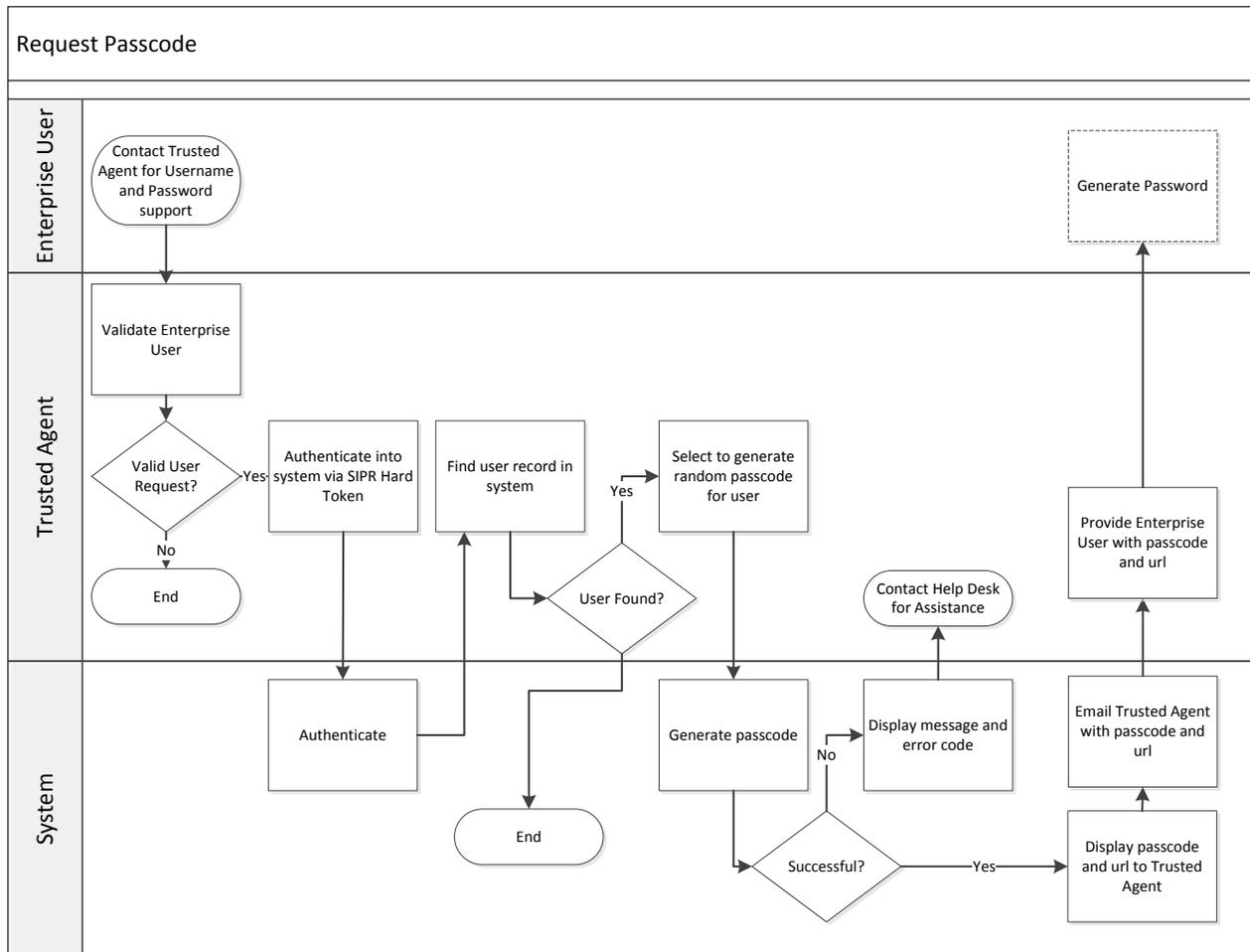


Figure 1 - Process - Generate Passcode

The Enterprise User requests the assigned Trusted Agent to use the system to generate a reset passcode. First, the Trusted Agent validates the User's identification and request. Next, the Trusted Agent authenticates into the system via SIPRNet Token. After authentication, the Trusted Agent finds the user via username and selects to generate a temporary passcode. Any issues the system encounters will result in an error code, that the Trusted Agent or User will reference for Help Desk requests.

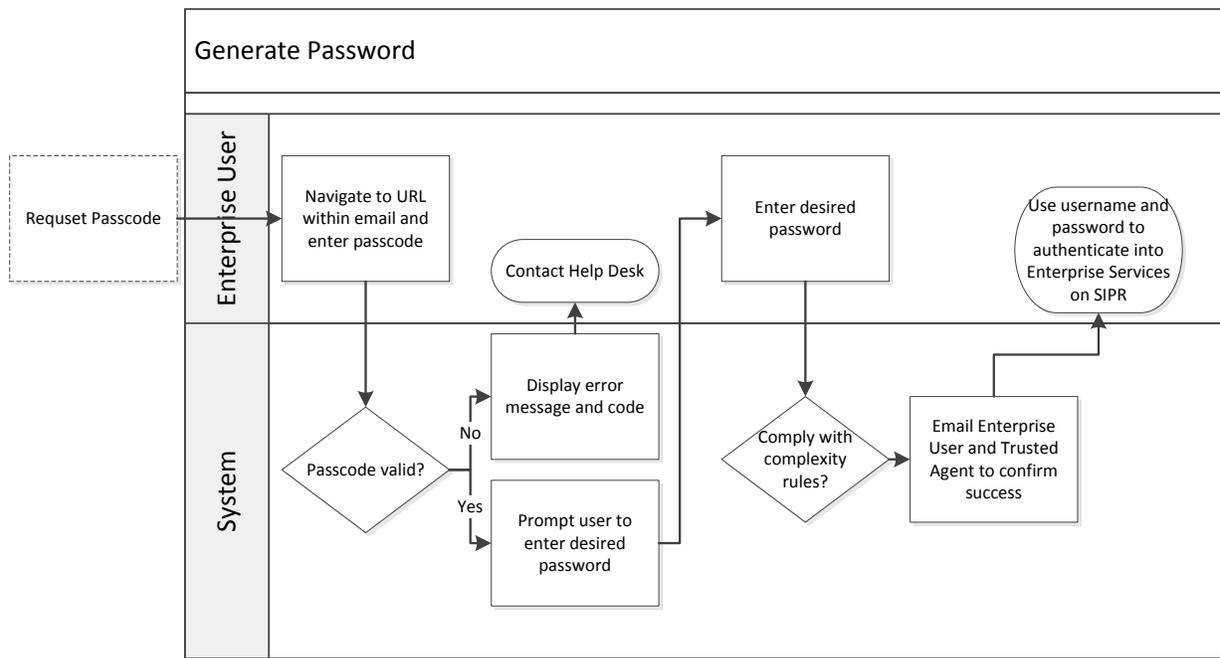


Figure 2 - Generate Password

Once the Enterprise User receives the temporary, randomly generated passcode, the User authenticates into the system to generate a new password. The password must comply with complexity rules.

ID Verification

Trusted Agents must verify the Enterprise User’s identity before using the solution to generate a passcode. Mission Partners will define the local ID verification process activities followed.

Provisioning Trusted Agents

Trusted Agents will be submitted to the IdSS/EASF Team for provisioning or deprovisioning following the formal Provisioning Process via DEPO. Reference the *DEPO Manager’s Guide* for details.

Internal Operations

The Username and Password solution will be hosted out of the San Antonio (SATX) DECC facility, with a failover site hosted in Mechanicsburg (MECH) DECC. Patching and maintenance will be performed by DECC staff.

Deployments

Routine patches and server maintenance will be performed by DECC personnel. However updates to the software solutions will be performed by the IdSS/EASF Development Team. All updates must comply with DoD Enterprise Email (DEE) configuration management processes, including submitting a formal Change Request. For more information reference the *IdSS/EASF Configuration Management Plan*.

Fail Over

A failover site will be maintained in the MECH DECC. Specific instructions for failover can be referenced in the *IdSS/EASF Disaster Recovery Plan*.

Configuration and Change Management

Configuration and Change Management will comply with the *IdSS/EASF Configuration Management Plan*.

Continuous Service Improvement

Enhancements

All requests for solution updates and new functionality must be submitted to the IdSS/EASF Configuration Manager. Enhancement Requests are reviewed for approval by the IdSS/EASF Configuration Control Board. If approved, Enhancement Requests are assigned to a software release for development and deployment. More details can be found in the *IdSS/EASF Configuration Management Plan*.

Bugs and Issues

The Help Desk will be the first level of support when end-users encounter issues in the system. For all system-related errors, the Username and Password solution will generate an error code to help the Help Desk identify the issue and solution. Major bugs that the Help Desk may not be able to address can result in a submission of an Enhancement Request.

Appendix A – Acronyms

CONOPS	Concept of Operations
DECC	Defense Enterprise Computing Centers
DEE	Defense Enterprise Email
DEPO	DECC Provisioning Online
DoD	Department of Defense
EASF	Enterprise Application Services Forest
ID	Identification
IdSS	Identity Synchronization Service
GAL	Global Address List
MECH	Mechanicsburg, PA
PKI	Public Key Infrastructure
SATX	San Antonio
SIPRNet	Secret Internet Protocol Router Network