Symantec™ by Broadcom

WHITE PAPER

Integrating with Electronic Identification and Trust Services

WHITE PAPER

Integrating with Electronic Identification and Trust Services

TABLE OF CONTENTS

Overview

The European Union Regulation (EU No. 910/2014) on electronic identification and trust services (eIDAS) enables businesses, citizens and public authorities to carry out secure and seamless electronic interactions. While digital identity (eID) programs were being implemented by countries across the EU, there was no interoperability between these different eIDs. The eIDAS regulation defined a common format to translate and share citizen identity data so that it could be understood and used across member states. This allowed citizens to prove and verify their identity when accessing online services in different member states using their own national eID.

The regulation led to the establishment of the eIDAS network, which consists of a series of eIDAS nodes implemented at the member state level. An eIDAS node can act as either a requester or as a provider of cross-border authentication. The eIDAS regulation also presents an opportunity for any organization to extend its goods and services to any EU citizen if they can integrate their applications and services into one of these eIDAS nodes. This white paper demonstrates how customers can leverage Symantec® SiteMinder™ to integrate into this European digital identity environment.

Introducing Symantec® SiteMinder™

The cornerstone for securing access to any online application or service is sufficient trust in a user's identity. From its initial development, SiteMinder was designed to secure the modern enterprise by delivering unified access management across any application for any user from any device. Leveraging Zero Trust principles, access to any SiteMinder-protected resource executes a three-step assessment:

1. Is the resource protected?
2. Is the user appropriately authenticated?
3. Is the user authorized?

The solution is the foundation for any Identity Fabric, because it applies the appropriate authentication mechanism to positively identify users, provides single sign-on and identity federation for seamless access, enforces granular security policies to stop unauthorized access to sensitive resources, and monitors and manages the entire user session to provide improved auditing and accountability.

SiteMinder Federation Support

A critical aspect for a modern Identity Fabric is the ability to enable federation, which allows users to move securely and seamlessly across devices and applications without any friction. In the context of the eIDAS network, SiteMinder enables your organization to weave both internal and external identity providers and service providers into your fabric, which improves the digital experience and user satisfaction. This is achieved through the native support for open standards, including OpenID Connect, OAuth, SAML, and WS-Federation. In fact, SAML is the principle protocol used across the eIDAS nodes; however, there are some caveats.

Understanding How eIDAS Works

Within the SAML specification, there are a number of mandatory and optional fields that can be used to exchange information. Although a successful federation transaction can be achieved using just the mandatory fields, most organizations also leverage one or more of the optional fields. This is especially true within the eIDAS network. The attributes needed to integrate the SAML token with the eIDAS nodes is defined within the eIDAS metadata. The metadata is an XML representation of the SAML configuration on both the Identity Provider and Service Provider sides, and can easily be imported into SiteMinder using the native federation tools. However, there are additional attributes that first may be needed to integrate to the national digital identity infrastructure.

eIDAS METADATA CAN CAN EASILY BE IMPORTED INTO SITEMINDER USING THE NATIVE FEDERATION TOOLS

To illustrate this, we have provided a detailed example of how to integrate SiteMinder with the digital identity infrastructure in Italy. These steps are essentially the same for each member state, but the metadata, certificates, and other configuration details may differ from country to country. Please refer to your country's digital identity program for their specific eIDAS integration requirements. A complete list of national eID and eIDAS nodes is kept by the European Commission.

A Practical Example: The Italian Digital Identity Environment

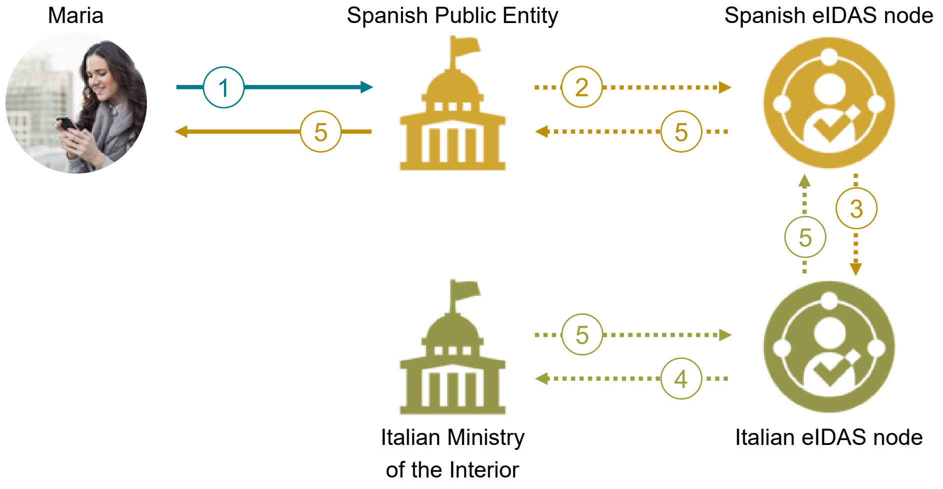
In response to the EU eIDAS regulation, the Italian government established the Sistema Pubblico di Identitià Digitale (SPID). The SPID consists of an open set of public and private entities who created an authentication system that allows Italian citizens and businesses to access online services with a unique digital identity. The SPID system has been accredited by the Agency for Digital Italy (AgID), which manages the Italian eIDAS node, as well as the registration and provisioning of credentials and online access tools services for citizens and businesses on behalf of public entities. In addition, there are two digital credentials that are part of the national Italian digital environment:

- **Electronic Identity Card (CIE):** One member of the SPID system is the Italian Ministry of the Interior. This public entity issues an electronic identity card (CIE) to Italian citizens. The CIE combines physical and digital security elements in a single credential that ensures the maximum level of confidence and accuracy in the process of ascertaining people's identities. The CIE is recognized in Europe as an eIDAS-compliant eID. In this case, the Ministry of the Interior serves as an Identity Provider, so when CIE is used to access any eIDAS-compliant online application or service in any member state, the authentication request will be routed to the Ministry of the Interior to validate the user's identity.

- **National Card Service (CNS):** Another digital identity that is supported by the SPID system is the National Service Card (CNS), which is issued by the Italian Ministry of Economy and Finance. The CNS is a physical smart card that uses an asymmetric encryption system similar to the CIE to guarantee the authenticity of the card. The user's identification data is stored inside the card in a similar fashion to the CIE; however, this card requires a smart card reader and local process to validate the keys used for authentication.

The CIE and CNS are both part of the SPID, and all three are integrated with the Italian eIDAS-node, which is operated by the AgID. The Italian eIDAS node serves as an authentication broker, acting as both as an Identity Provider for Italian citizens who are accessing a foreign online service, and as a Service Provider for foreign users who need to access an Italian online service. Consider the example below.

Figure 1: eID Authentication Example



Maria, an Italian citizen, wants to report her new address to a Spanish Public Agency. To do this, she must authenticate herself to the site and Maria wants to use her CIE credential. The authentication process follows these steps:

1. Maria visits the website for the Spanish public agency and selects the eIDAS authentication button to be redirected to the Spanish eIDAS node.
2. The Spanish public agency redirects Maria to the Spanish eIDAS node, where Maria then selects Italy as the member country where she wants to authenticate.
3. The Spanish eIDAS node transmits the request to the eIDAS node in Italy and Maria is redirected to the Italian site.
4. The Italian eIDAS node prompts Maria for her Italian SPID or CIE credentials. In this case, Maria selects CIE and is redirected to the Italian Ministry of the Interior.
5. Maria is prompted for her CIE credential, which is validated. The Ministry sends the verified identity to the original requestor, the Spanish public administration, through the eIDAS nodes, which gives Maria access to the online service.

EACH COUNTRY MAY HAVE THEIR OWN SPECIFIC eIDAS INTEGRATION REQUIREMENTS

The eIDAS infrastructure provides the infrastructure to support federation across member states, and the Agency for Digital Italy (AgID) supervises the mechanisms for provisioning the CIE or SPID account to Italian citizens, as well as handling the actual authentication verification of all Italian and EU citizens. Similarly, France-Connect/SGNI, Clave, and BMI provide identical capabilities to French, Spanish, and German citizens respectively, enabling them to use electronic citizen ID and other strong authentication mechanisms supported by member states. Therefore, organizations can leverage SiteMinder native identity federation capabilities to easily integrate with the eIDAS network to act as either a Service Provider or an Identity Provider, or both. The configuration steps required for this integration are provided below. Configuration steps may vary across member states.

ORGANIZATIONS CAN LEVERAGE SITEMINDER NATIVE IDENTITY FEDERATION CAPABILITIES TO EASILY INTEGRATE WITH THE eIDAS NETWORK TO ACT AS EITHER A SERVICE PROVIDER OR AN IDENTITY PROVIDER, OR BOTH.

Step 1: Configuring the Federation Certificates

One of the first steps in defining a federation within SiteMinder is to establish the digital certificates required to sign the SAML exchanges. Within the SPID system, these certificates must be compliant with the AgID regulations. The standard certificates generated by SiteMinder are not compliant. The AgID provides a tool that can generate SPID-compliant certificates, which can be uploaded into SiteMinder through the console and used for federation.

Step 2: Importing the SAML Metadata

The metadata is an XML representation of the SAML configuration both on the Identity Provider and the Service Provider sides. In Italy, the AgID has defined which optional statements and extensions of the protocol are needed in order to conduct a successful federation transaction within the SPID system. The AgID publishes the list of all the metadata all of the registered entities in the SPID registry.

The AgID has published technical rules to allow organizations to configure their SiteMinder environments to act as an Identity Provider, a Service Provider, or an Attribute Authority using the SAML protocol within the SPID system. Additional constraints are required when an organization wants to support the CIE as an authentication credential. There are a few additional attributes required for the eIDAS network. Fortunately, the AgID has provided an incremental approach, so it is possible to define a unique configuration that is accepted by all authentication mechanisms at both the Identity Provider and Service Provider levels.

When configuring SiteMinder as a Service Provider, you must download the metadata of all the Identity Providers and then upload this information into SiteMinder as Remote Identity Provider. At the same time, you must also create a Local Service Provider for managing the local application. Then you create a Partnership between the application and all of the Identity Providers. You also need to download the metadata to support the CIE credential and eIDAS node, and upload this information into SiteMinder.

SITEMINDER ENABLES YOUR ORGANIZATION TO WEAVE BOTH INTERNAL AND EXTERNAL IDENTITY PROVIDERS AND SERVICE PROVIDERS INTO YOUR FABRIC, WHICH IMPROVES THE DIGITAL EXPERIENCE AND USER SATISFACTION.

Once you have finished configuring SiteMinder, use the standard feature to generate and download the metadata implemented for the Service Provider. This information should be registered in the AgID site; however, to comply with AgID requirements, the following changes are required:

- Modify some attributes to comply to specific rules, as described above.
- Add the Organization statement (optional in SAML) to describe the entity providing the service.
- Add the Contact statement (optional in SAML) to identify the contact person responsible for this service.

The same metadata file could be used both for CIE and the Italian eIDAS node, but in this case additional attributes (CIE metadata, eIDAS metadata) are required for the systems.

Once these changes are made, you must sign the new metadata file using the metadata signing tool provided by the AgID. Before registering the metadata, the AgID provides an open source tool that can be used to verify the correct definition of the SAML token.

Step 3: Creating a Compliant Web Interface

Although the creation of the login page is out of scope for the SiteMinder solution, this is a critical element for simplifying the user experience. The AgID does provide an open source tool that can be used to generate a compliant login page. In addition, the AgID has defined a set of guidelines for login pages, icons, and buttons to ensure that users have a consistent experience across all Identity Providers and Service Providers. Similarly, there are guidelines for displaying the CIE button and eIDAS button.

Summary

The Italian SPID system and eIDAS nodes provide a simplified way to safely publish a web application to all EU citizens. Additionally, organizations can eliminate the need to manage the registration of users and provisioning of credentials by leveraging the national eID. Leveraging the standard SiteMinder Identity federation capabilities to integrate with this infrastructure enables customers to improve security by eliminating the need to store credentials, reduce the cost for managing users, and increase revenues by offering services to more users.

For more information, visit our website at: www.broadcom.com

SYM-SM-EID-WP100 December 21, 2023