



(NETW 1002)

Systems and Network Security Milestone 3 Submission Report

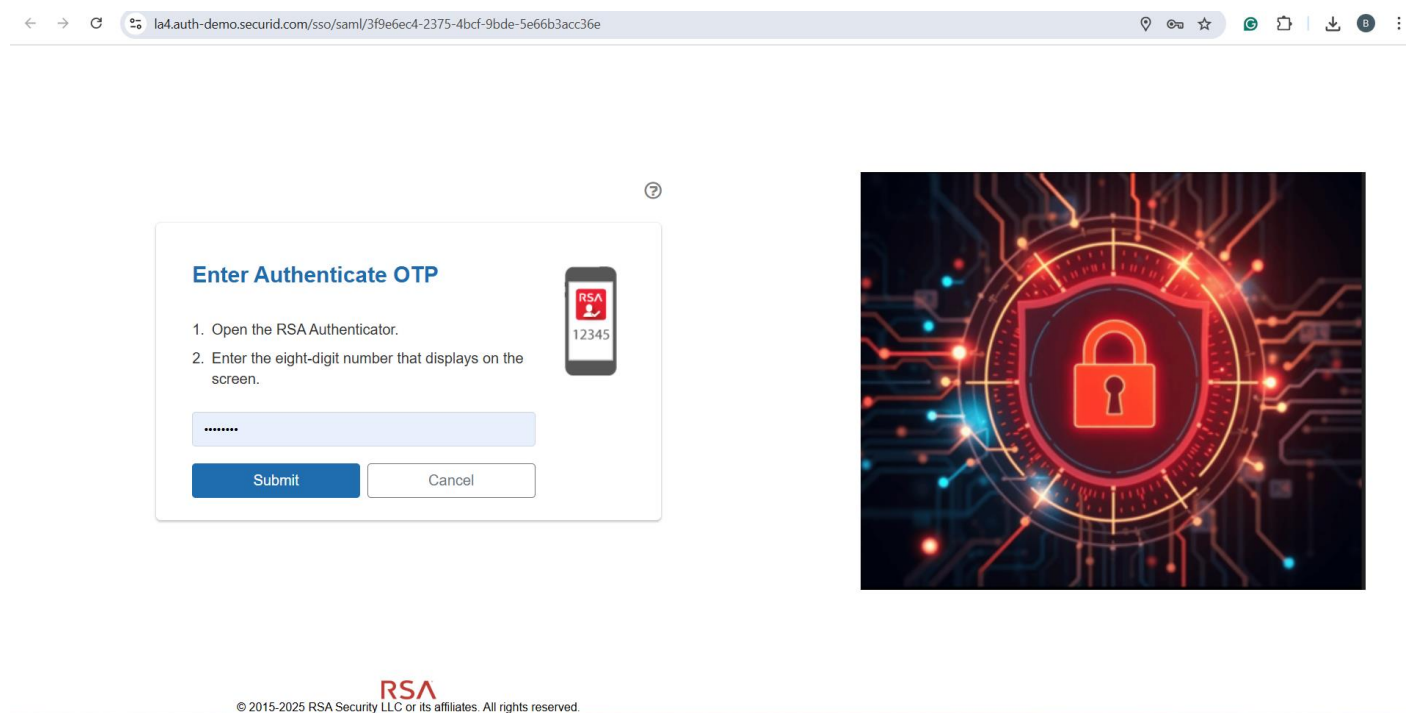
OWN YOUR
IDENTITY.

Milestone 3 Report Submission:

Milestone 3 Screenshots:

1. Configuring IdP-initiated application

*** **FIRST SCREENSHOT:** Capture the Authenticate OTP prompt after clicking on the application in MyPage.



*** **SECOND SCREENSHOT:** Take a full-page screenshot, including the URL, showing the confirmation message at the SP after successful authentication.



Hello boules.ghaly

You successfully federated into this demo site!
Below you'll find additional information about the SAML assertion that brought you here.



Subject Information

Information about the Subject (the user) that got federated

Subject

NameID

boules.ghaly

Attribute	Value
Format	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified



Authentication Details

All information about how the identity authenticated at the identity provider

AuthNStatement

Attribute	Value
AuthNInstant	2025-05-06T10:59:06.051Z
SessionIndex	_ec442186ac84c436

AuthNContext

AuthNContextClassRef

urn:rsa:names:tc:SAML:2.0:ac:classes:spec:SAML Access Policy:low



Attribute Details

No attributes found in SAML assertion



Assertion Details

The "everything else of some interest" section

Attribute	Value
StatusCode	urn:oasis:names:tc:SAML:2.0:status:Success
Issuer (Entity ID)	https://ia4.auth-demo.securid.com/sso/saml/3f9e5ec4-2375-4bcf-9bde-5e56b3acc26e
Assertion ID	_ec442186ac84c436
IssueInstant	2025-05-06T10:59:15.155Z
Hashing Algorithm	SHA256

Conditions

Attribute	Value
NotBefore	2025-05-06T10:58:15.155Z
NotOnOrAfter	2025-05-06T11:05:15.155Z

AudienceRestriction

IAMShowcase

[SHOW SAML ASSERTION](#)[Legal](#)

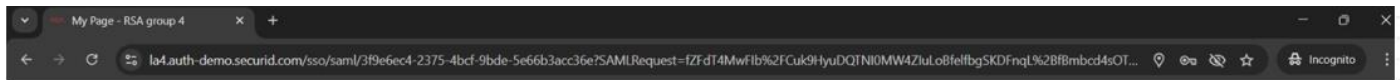
- [TM Trademarks](#)
- [Privacy Policy](#)

[Links](#)

- [Report a Problem](#)
- [RSA Homepage](#)
- [RSA SecurID / ID Plus](#)

2. Configuring SP-initiated application.

*** **THIRD SCREENSHOT:** Capture the Password + Authenticate OTP prompt upon accessing the URL.

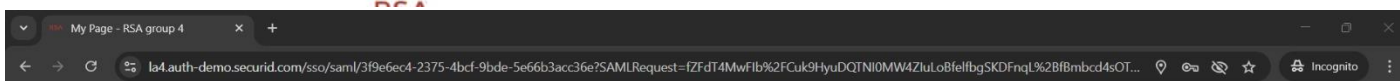


Enter User ID and Password

User ID
boules.ghaly

Password

Submit Cancel



Enter Authenticate OTP

1. Open the RSA Authenticator.
2. Enter the eight-digit number that displays on the screen.

12345

Submit Cancel

Show more



*** **FOURTH SCREENSHOT:** Take a full-page screenshot, including the URL, showing the confirmation message after successful authentication.



Hello boules.ghaly

You successfully federated into this demo site!
Below you'll find additional information about the SAML assertion that brought you here.



Subject Information

Information about the Subject (the user) that got federated

Subject

NameID

boules.ghaly

Attribute	Value
Format	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified



Authentication Details

All information about how the identity authenticated at the identity provider

AuthNStatement

Attribute	Value
AuthNInstant	2025-05-06T10:49:58.583Z
SessionIndex	_97a6b3b22ac7d638

AuthNContext

AuthNContextClassRef

urn:rsa:names:tc:SAML:2.0:ac:classes:spec:SAML Access Policy:low



Attribute Details

No attributes found in SAML assertion



Assertion Details

The "everything else of some interest" section

Attribute	Value
StatusCode	urn:oasis:names:tc:SAML:2.0:status:Success
Issuer (Entity ID)	https://la4.auth-demo.securid.com/sso/saml/3f9e6ec4-2375-4bcf-9bde-5e66b3acc36e
Assertion ID	_97a6b3b22ac7d638
IssueInstant	2025-05-06T10:50:00.633Z
Hashing Algorithm	SHA256

Conditions

Attribute	Value
NotBefore	2025-05-06T10:49:00.633Z
NotOnOrAfter	2025-05-06T10:56:00.633Z

AudienceRestriction

IAMShowcase

[SHOW SAML ASSERTION](#)



Legal

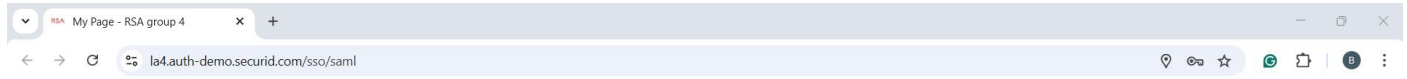
- [TM Trademarks](#)
- [Privacy Policy](#)



Links

- [Report a Problem](#)
- [RSA Homepage](#)
- [RSA SecurID / ID Plus](#)

***Bonus step: Make the application accessible from MyPage while it's SP-initiated.:



Enter User ID and Password

User ID

boules.ghaly

Password

Submit Cancel



Enter Authenticate OTP

1. Open the RSA Authenticator.

2. Enter the eight-digit number that displays on the screen.

12345

Submit Cancel

Show more



3. Comparison.

- provide a **comparison of the authentication flows** between **SP-initiated** and **IdP-initiated mechanisms**.

Feature	SP-Initiated Authentication	IdP-Initiated Authentication
Initiating Party	Service Provider (SP)	Identity Provider (IdP)
Authn. Flow	<ol style="list-style-type: none"> 1. User accesses SP through the link provided, this initiates SAML AuthnRequest to the IdP. 2. SP send AuthnRequest to the IdP and redirects user to the IdP 3. IdP authenticates user using username and password. 4. User is then prompted to enter an OTP from the authenticator app. 5. If both credentials and MFA succeed, the IdP generates a SAML Response and sends it to the SP. 6. SP verifies the SAML Response and grants access 	<ol style="list-style-type: none"> 1. User accesses IdP portal (mypage) 2. IdP (mypage) authenticates user using primary auth (user + password) then a step up authentication (push notification and approve on mobile phone) 3. user clicks on the application 3. IdP sends SAML response to SP 4. SP requires another MFA (Authentication OTP from the app on the phone) 5. SP grants access
User Experience	Starts from the RSA Demo app (typing the url of the app in the portal taken from the IdP metadata)	Starts from my page
SAML Request	Sent by SP to IdP	Not required (unsolicited SAML response from IdP)
SAML Response	Returned from IdP to SP after authentication	Directly generated by IdP after login
Use Case Suitability	Best when users directly access apps	Best for SSO portals like mypage

RSA