Entrust-SSL.com Partnership

Path To Deliver Public TLS/SSL Certificates After Oct 31, 2024

Entrust is committed to transparency and sharing information quickly with our customers on our partnership with SSL.com.

Please note: this presentation represents Entrust's best knowledge and expectations at the time of this webinar. Some information presented is subject to review and approval as part of a WebTrust audit.

Aug 2024

ENTRUST

SECURING A WORLD IN MOTION

How We Will Issue SSL.com TLS Certificates Overview

Customers will continue to use the ECS portal or ECS API

- Entrust will connect via API with SSL.com to complete domain verifications and request, pickup TLS certificates

Entrust will act as a delegated RA for SSL.com

- Organizational validation will be performed by Entrust
- Domain validations will go through Entrust to SSL.com

Customers will remain eligible to issue TLS certificates in accordance with their purchased entitlements before and after Oct 31, 2024

- Up to Oct 31, 2024: TLS certificates issued by Entrust
- After Oct 31, 2024: TLS certificates issued by SSL.com (Entrust TLS will remain available)

ENTRUST

How We Will Issue SSL.com TLS Certificates Overview

After 31 October 2024

- Buy from Entrust, ECS
- Entrust pricing & agreements

- Support single point of contact

- Use Entrust ECS
- Re-use of Entrust verification work; re-validation may be required

- ECS portal, Cert Hub
- Persistent API connections (Venafi etc), 3rd party cert visibility, reporting

- No revocation of Entrust certs required
- Support of contracted certs

- SSL.com issued certificate from Entrust ICA
- Org and Domain validation initiated through Entrust ECS portal, domain validation performed by both SSL.com and Entrust, org validation performed by Entrust

No Change

Limited Change

ENTRUST

New Solution Supported by Google, Mozilla, and Customers

Google update **July 22, 2024**

"**Website operators who will be impacted** by the upcoming change in Chrome for new TLS certificates issued after October 31, 2024 **can explore continuity options offered by Entrust**."

Mozilla posted **July 30, 2024**

"**We are aware that Entrust has reached an agreement with SSL.com** to act as its External Registration Authority (RA), performing pre-issuance vetting of certificate applicants for SSL.com. **We support this arrangement…**"

- Global financial institution
- Large European bank
- European oil producer
- Global sporting goods company
- US food processing company
- US healthcare insurance provider
- Large home/auto insurance company
- US cable/communications provider

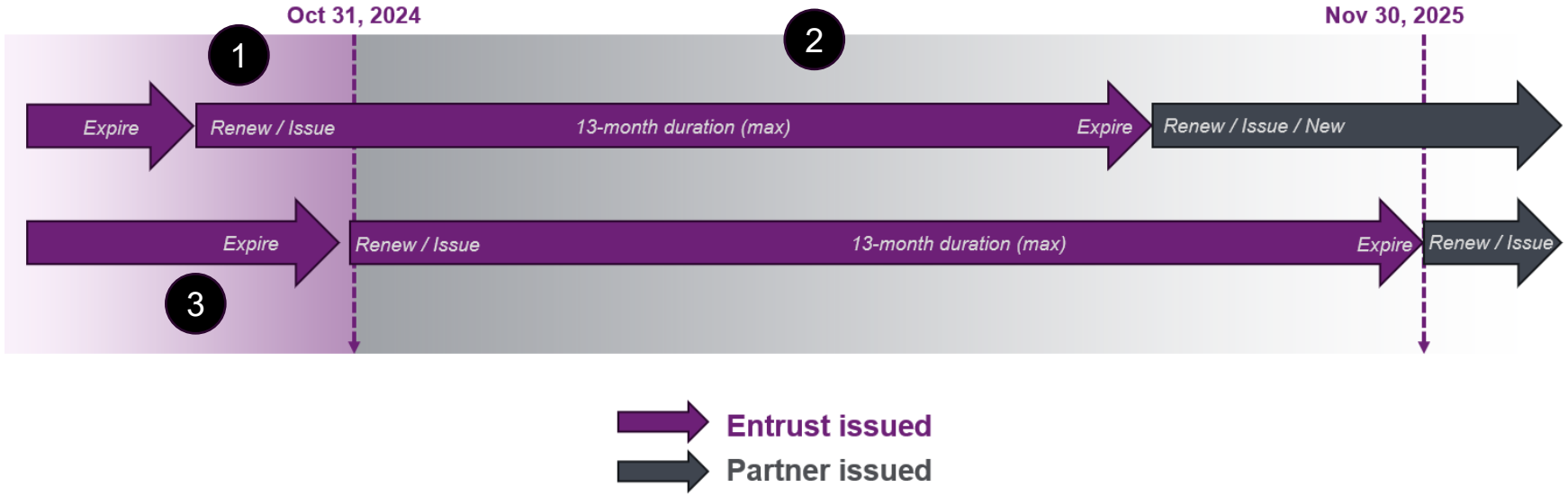
ENTRUST

Timeline of Entrust vs SSL.com Certificate Issuance

1. **Issued Entrust public TLS certs** will be trusted by the browsers until their expiry date

2. **Entrust partnering with SSL.com** to issue certs post 31 Oct

3. **Recommendation:** For customers with unique testing requirements or use cases renew TLS certs prior to Oct 31 that are expiring within 3-6 months of Oct 31, 2024



Key Dates for Customers

Aug 21/22: Attend webinar

Sept 30: Targeted ECS release with SSL.com integration

- Start issuing certificates from new hierarchies
- Configure clients and start domain re-verification
- Issue production certificates from SSL.com

Oct 31: ECS defaults to SSL.com

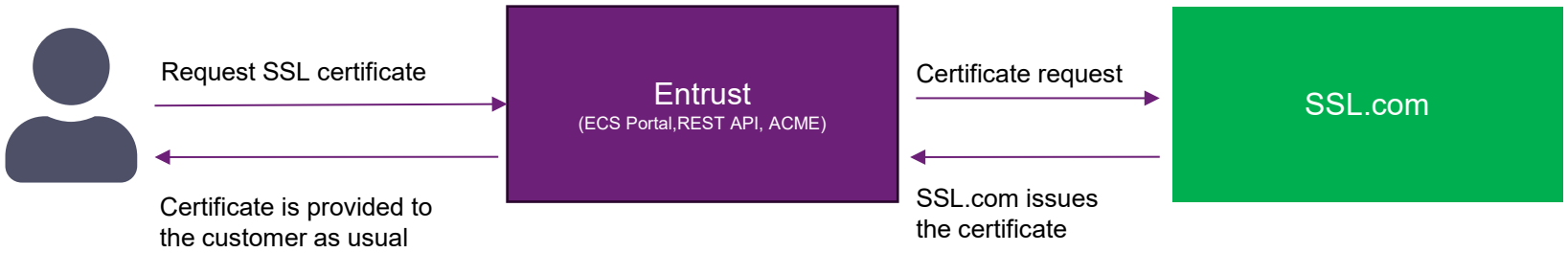
ENTRUST

Technical Details

Public TLS/SSL Certificate Issuance

- TLS/SSL Certificate Issuance Flow
  - Public SSL certificates will continue to be created from the Entrust Certificate Services (ECS) portal or ECS REST API
  - Certificates will be delivered to the requester by Entrust
  - Full certificate lifecycle management (new, reissue, revoke, renew) managed by ECS
  - ECS licenses are still valid and consumed by this process
  - No delay in certificate issuance is expected

- **As of Oct 31, 2024, SSL.com will be the default issuing CA for Public SSL certificates**
  - Default issuance path will be SSL.com, however, the issuing TLS CA can be overridden with Entrust for non-traditional TLS use-cases (where browser-trust is NOT required)



ENTRUST

Testing Certificates from SSL.com

- The SSL.com roots that will sign certs from ECS are on the Root Hierarchy slides
  - **Customers can confirm that the roots are included in their browsers or other root stores**

- **We are targeting a release for the end of September 2024** that will enable customers to test & start using the new certificates and updated issuance path, including:

  - Start re-verifying domains with Entrust and SSL.com
  - Issue SSL.com certificates from the ECS UI and API, while still being able to issue certificates from Entrust
  - Issued certificates will be signed by the new CA Hierarchy (see CA Hierarchy slide)
  - These certificates will be fully valid production certificates!

ENTRUST

Certificate Issuance Support After October 31, 2024

Buy, Renew, Support

Buy Certs *(Phone)*
Net New, Add, Renew

Add More
(Self-serve Store)

Resellers
(Partner Portal)
Net New, Expand, Renew

Sales & Support
Single point of contact

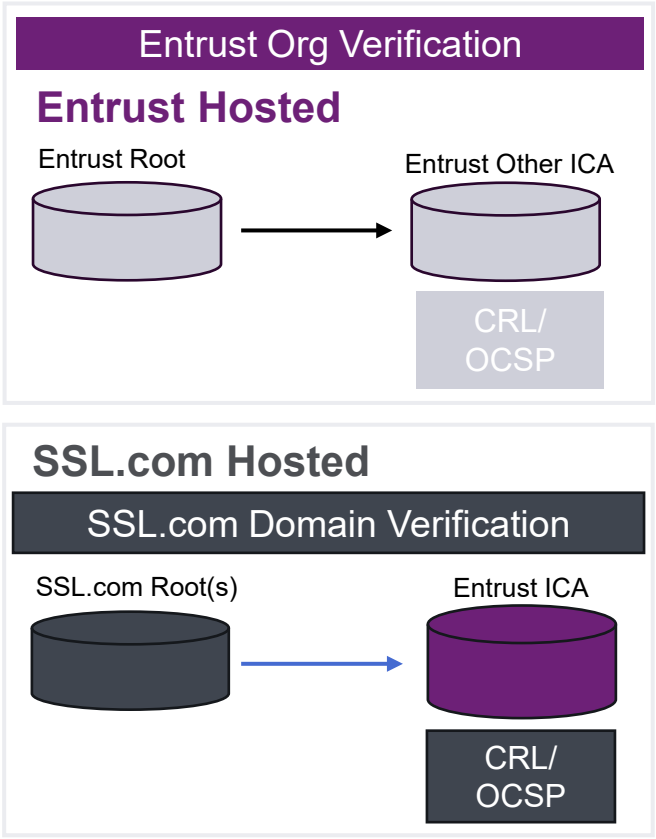
Management Portal

Entrust Certificate Services

- Cert Lifecycle Management
- Request domain validation
- Request Org validation
- Request Certificates UI
- Request Certificates API
- Reporting

VMC, SMIME, Code Sign, Doc Sign, QWAC PSD2, Non-trusted Entrust certs, Client-Auth certs

OV/EV TLS Trusted Certificates



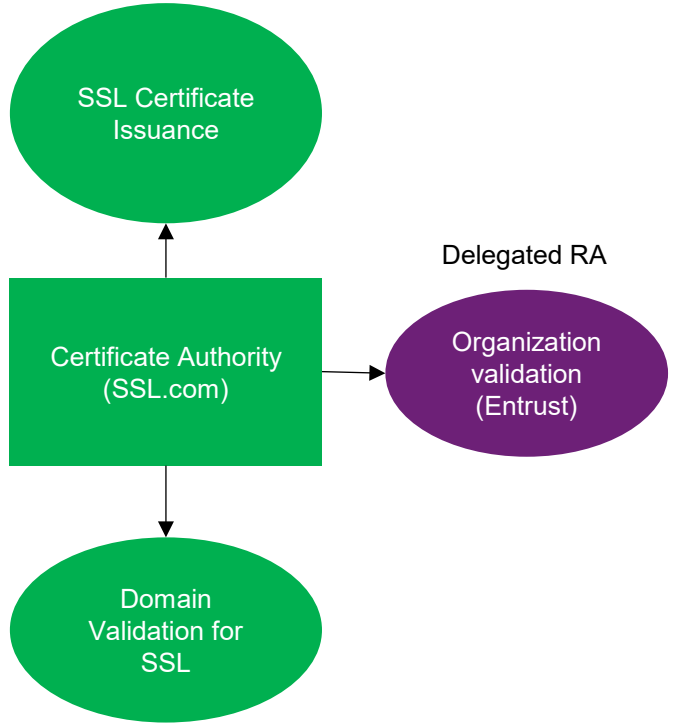
No change to:

- *Your Entrust pricing*
- *Your single point of contact*

ENTRUST

Entrust will Continue as the Registration Authority for TLS/SSL Certificates

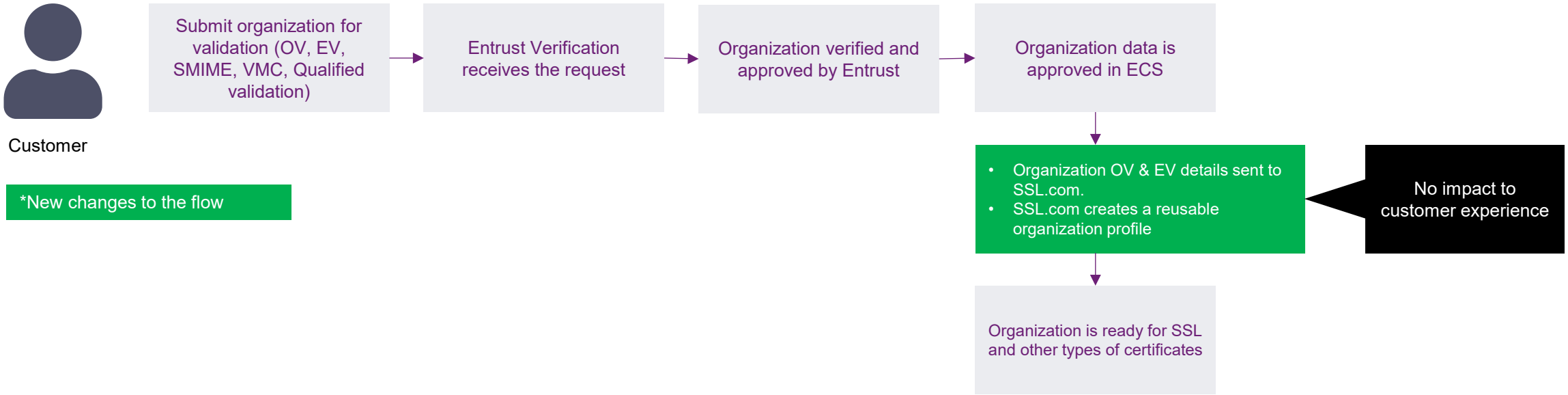
- A Delegated Registration Authority (RA) is an entity that a Certificate Authority (CA) authorizes to perform the validation and vetting processes necessary for issuing digital certificates.
- SSL.com (CA) will delegate vetting of organization & certificate requests to Entrust (Delegated RA) for issuance of **Public SSL certificates**
- Domain validation cannot be delegated to RA – SSL.com will verify domains



This approach is supported by the CA/Browser Forum Baseline Requirements, and by Chrome & Mozilla

ENTRUST

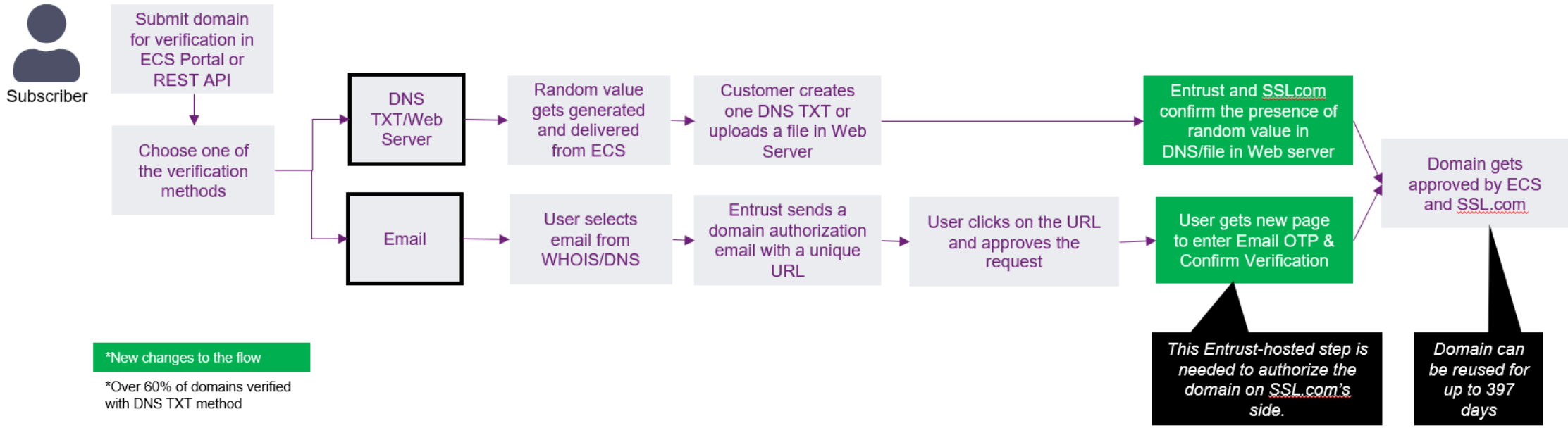
Organization Validation Flow (No Change for Customer)



- Organizations will continue to be managed via the Entrust Certificate Services (ECS) Portal
- Entrust will continue to perform organization validation – no changes to current flow
- Existing verified organizations/clients will remain valid - no changes to current flow

ENTRUST

Domain Validation Flow (Limited Change for Customer)



- Domains continue to be managed via the ECS Portal, using the available automated methods
- ***Domains must be re-verified through our new flow (in October)*** to continue issuing TLS certificates. Bulk domain verification tools still available in ECS.
- Domain Validation screen will show who validated
- Domains will continue to be re-verified every 398 days

ENTRUST

Initial Configuration for SSL.com

1. Update each ECS client to support SSL.com
   - Acceptance of new Subscriber Agreement
   - Selection of CA to issue certificates
     - <=Oct 31, 2024 – Customer may select Entrust (Default) or SSL.com and toggle between for testing SSL.com
     - >Nov 1, 2024 – Default changes to SSL.com and Customer may select toggle between if they wish to issue Entrust certificates for non-browser use cases
2. Re-validate domains through ECS
3. After these updates, ECS is ready to issue certificates

ENTRUST

User Interface:

- Domain Management changes
  - Modified email method for domain management per previous slides
  - New column in Domain management to reflect which CA has verified domain
- Reporting updates
  - New columns or values in fields to reflect the CA issuing

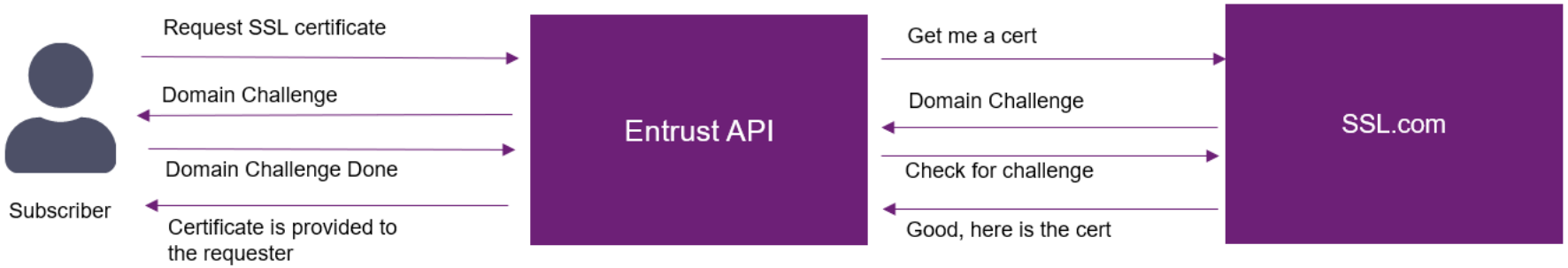
Only minor UI changes to certificate issuance in ECS

ENTRUST

API and ACME v2

API:

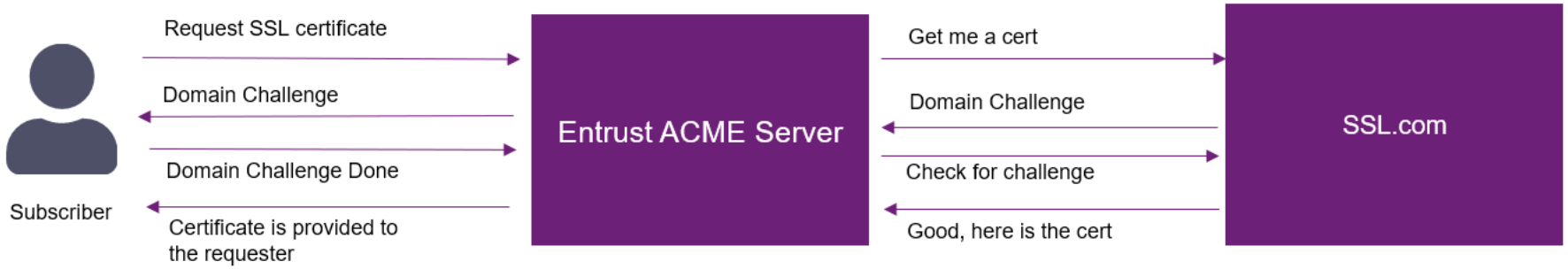
No configuration changes for customers - use existing Entrust API



ACME v2

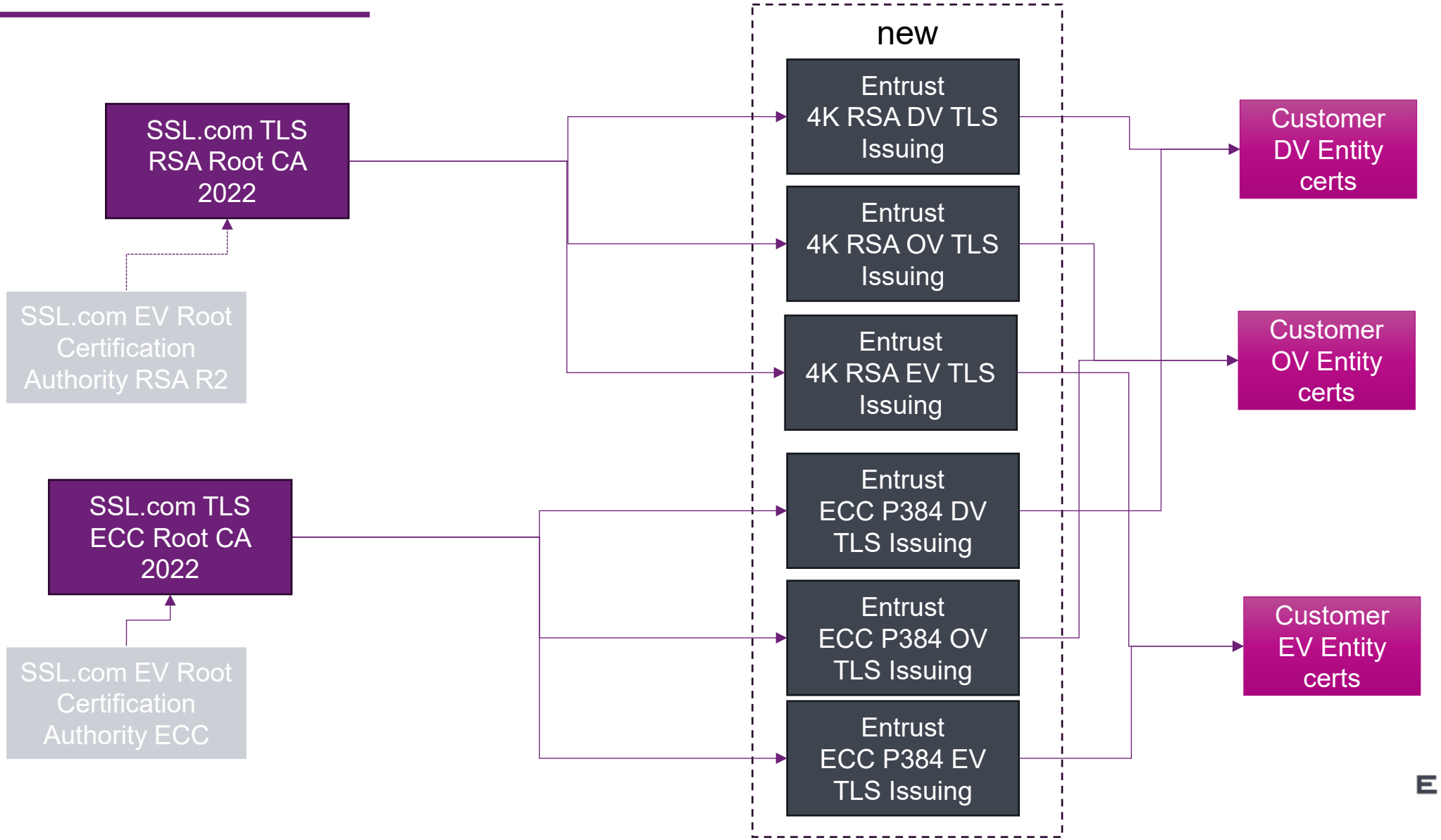
No configuration changes - use existing Entrust ACMEv2 server

New display column in External Account Binding



ENTRUST

New Root Hierarchy for TLS/SSL



ENTRUST

SSL.com Roots Detail

Common Name (CN)	Date	Key	Hash	Use Cases	Link
SSL.com TLS RSA Root CA 2022	2022	RSA 4096	SHA256	DV TLS + OV TLS + EV TLS	https://crt.sh/?caid=247168
SSL.com TLS ECC Root CA 2022	2022	ECC P384	SHA384	DV TLS + OV TLS + EV TLS	https://crt.sh/?caid=247167
SSL.com EV Root Certification Authority RSA R2	2017	RSA 4096	SHA256	DV TLS + OV TLS + EV TLS	https://crt.sh/?caid=51081
SSL.com EV Root Certification Authority ECC	2016	ECC P384	SHA256	DV TLS + OV TLS + EV TLS	https://crt.sh/?caid=30477

Finalizing plan with SSL.com on cross-certification of SSL.com Roots with Entrust Roots

ENTRUST

Certificate Authority Authorization (CAA)

Certificate Authority Authorization (CAA) is an optional security feature that allows domain owners to specify which Certificate Authorities (CAs) are authorized to issue certificates for their domains

- The “entrust.net” and “Affirmtrust.com” CA ID’s for CAA will work for both certificates issued by Entrust and those issued by SSL.com – no action is required
- Entrust Knowledge Base for CAA
  - Add CAA record to your DNS Zone
  - Add CAA record to hosted DNS

No changes to CAA

ENTRUST

Qualified TLS Certificates

- **QWAC PSD2 Certificates**
  - **No change. Still issued by Entrust.**
  - PSD2 certificates are used for server-to-server authentication and do not rely on trust from browser root stores.

- **QWAC EIDAS Certificates**
  - These certificates rely on global trust in the browser root store and will not be trusted if issued by Entrust after Oct 31, 2024
  - We recommend issuing all QWAC EIDAS certificates needed for the next year from Entrust prior to Oct 31, 2024 as they will remain trusted
  - After Oct 31, 2024 we will resell through a partnership with DTrust (as we did prior to becoming a QTSP), these certificates will not appear in your ECS portal

ENTRUST

Summary

Customers will continue to use the ECS portal or ECS API

- Entrust will connect via API with SSL.com to complete domain verifications and request, pickup TLS certificates

Entrust will act as a delegated RA for SSL.com, keeping the organizational verifications with Entrust – domain validations will go through Entrust to SSL.com

Customers will remain eligible to issue TLS certificates in accordance with their purchased entitlements before or after Oct 31, 2024

- Up to Oct 31, 2024 TLS certificates issued by Entrust
- After Oct 31, 2024 TLS certificates issued by SSL.com (Entrust TLS will remain available)

Aug 21/22: Attend webinar

Sept 30: ECS release with SSL.com integration

- Start issuing certificates from new hierarchies
- Configure clients and start domain re-verification
- Issue production certificates from SSL.com

Oct 31: ECS defaults to SSL.com

ENTRUST

Questions?

>> Please use the Q&A function to ask questions.

entrust.com

ENTRUST

SECURING A WORLD IN MOTION

Thank you!

entrust.com