



Symantec Authentication-Only Services

Authentication is a Symantec core competency

- Symantec has ~65% of the world's SSL business, and our capabilities to perform authentication and vetting are core competencies: nobody does this as well as we do, nor with our scalability
- Symantec already has access to over 200 databases globally, among the best known are:
 - Internet-related: WHOIS, ICANN, and IANA
 - Business-related: D&B and Experian
 - Government-related: US Government Denied Lists, Secretary of State, City and County business license databases, UK Companies House, Australia's ASIC, China's State Administration (for Industry & Commerce), etc.
 - Phone-related: Online Yellow Pages, directory assistance, etc
 - We add new databases frequently



Authentication is a Symantec core competency

- Some of our authentication processes are “database dips” -- and results are known in near real-time.
- Some processes are human-based (making verification phone calls, processing hardcopy documents, such as notarized letters, passports, professional opinion letters, billing statements, acknowledgement letters, etc.) – and these do not complete in real-time.
- We have the ability to customize our authentication processes: for example, we can do a “database dip” into a database that you manage (or another third party) in order to make a decision that includes data from both our systems and yours.



New member onboarding and authentication

- Many organizations have requirements to authenticate new members, customers, etc – but they are almost always manual processes
- Using Symantec's Authentication-Only Services allows you to leverage Symantec's substantial and ongoing investment in highly scalable and automated processes
- The workflow typically goes like this:
 - You send us (via our APIs) information and rules about organizations/individuals to be authenticated
 - We perform the authentications and return the results to you
 - Your application decides what action to take from there



Symantec and ESPC

- Symantec would like to engage with members of the ESPC to better understand
 - What authentication processes are now undertaken by ESPC members?
 - Can they be standardized? Or is each member unique?
 - What authentication needs to be done in realtime vs humantime?
 - What are the volumes of authentications that need to be done?
- Providing a conceptual proposal (for approval)
- Providing an implementation proposal (with pricing)





Thank you!

Geoffrey Noakes

geoffrey_noakes@symantec.com

+1-415-370-5980

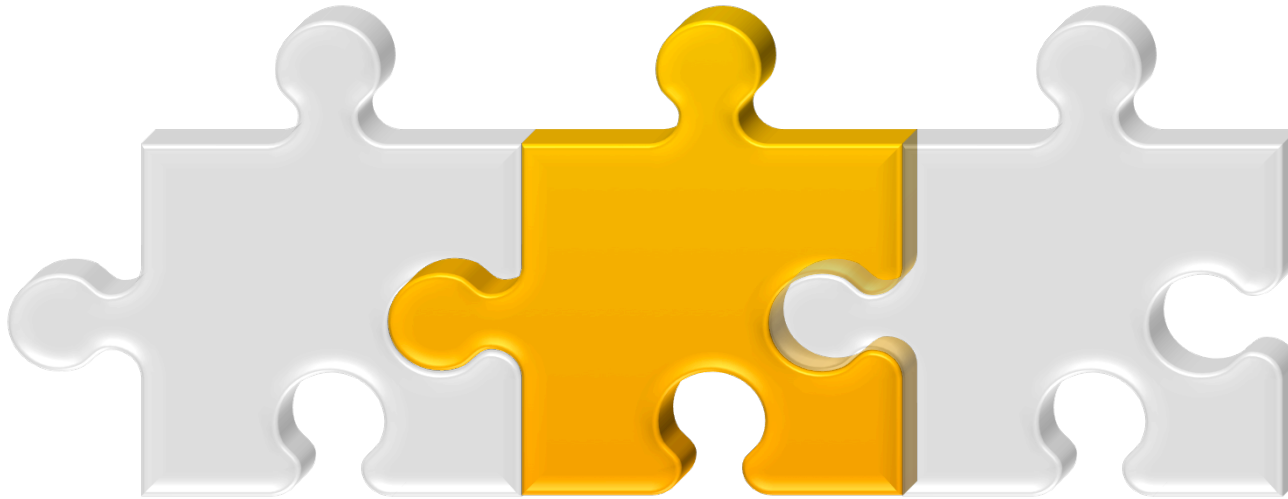
Copyright © 2013 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.

Backup slides (authentication on SSL certs)



Vetting Process: **Domain Validation**



Domain Validation

- Authenticate through public domain name registration (WHOIS)
- May require authorization from domain owner

Applicable to:

Domain Validated



Organization Validated



Extended Validation

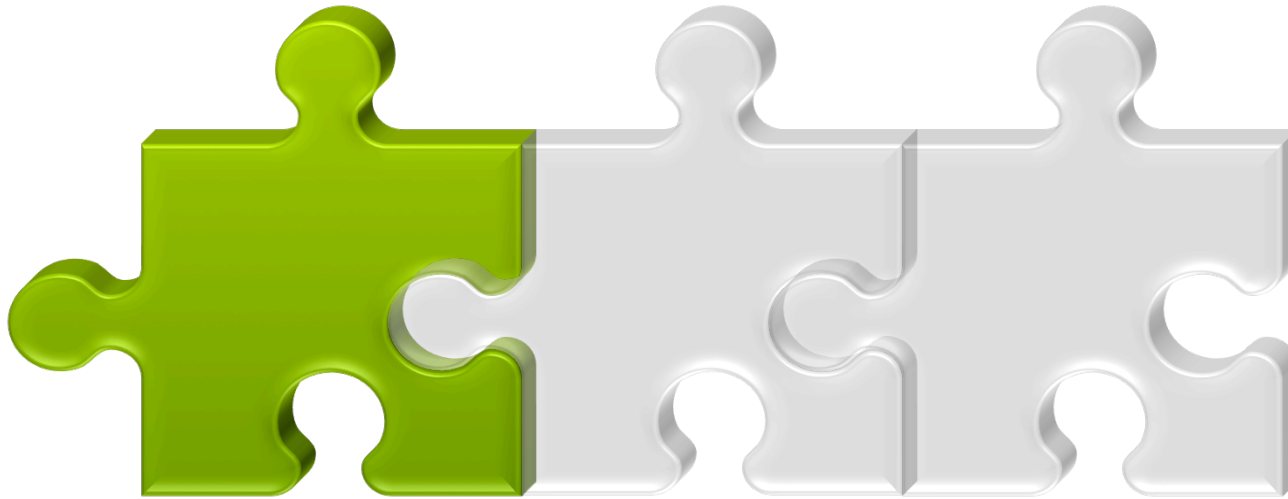


Code Signing

Symantec Safe Site



Vetting Process: **Organization Authentication**



Organization Authentication

- Verify organization name, jurisdiction, registration and good-standing
- Multiple resources and databases used

EV Requirements:

- Organization has the ability to engage in business
- Physical business address verification required

Applicable to:

Domain Validated

Organization Validated



Extended Validation



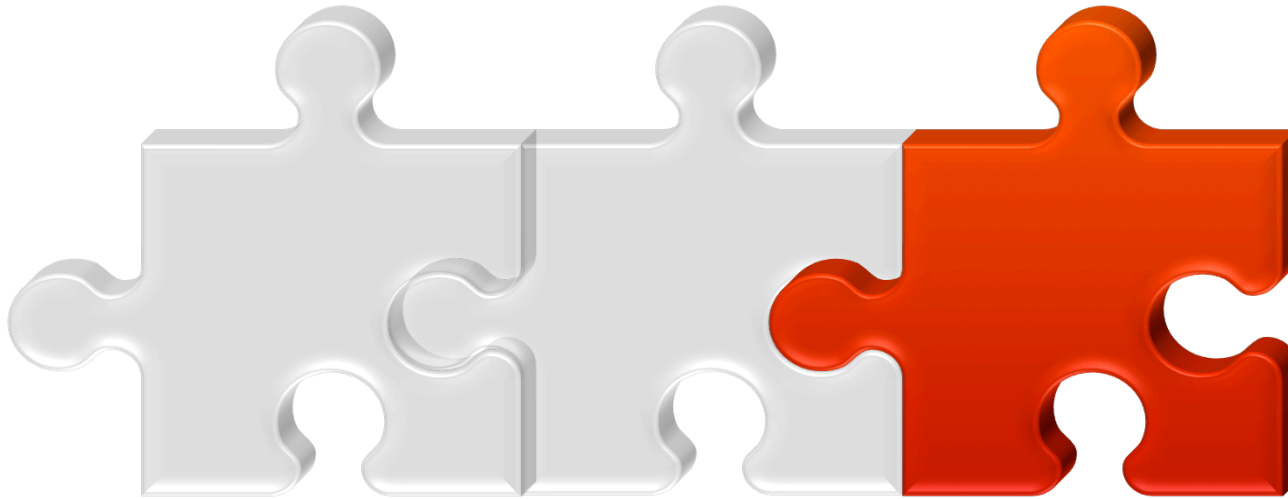
Code Signing



Symantec Safe Site



Vetting Process: **Corporate Contact Verification**



Corporate Contact Verification

- Verify corporate contact works for the company
- Uses 3rd party telephone listing

EV Requirements:

- Employment verification through human resources
- Corporate contact must have the “Authority” to purchase the EV certificate
- Acknowledgement Agreement

Applicable to:

Domain Validated

Organization Validated



Extended Validation



Code Signing



Symantec Safe Site

