NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

MULTIFACTOR AUTHENTICATION FOR E-COMMERCE

Online Authentication for the Retail Sector

The National Cybersecurity Center of Excellence (NCCoE) is addressing the challenge of fraud in e-commerce transactions through collaborative efforts with industry and the information technology community, including vendors of cybersecurity solutions. This fact sheet provides an overview of the *Multifactor Authentication for E-Commerce* Practice Guide, including background and challenge, goals, and potential benefits. If you have feedback on the architecture or the relevance and usefulness of this practice guide or would like to schedule a demonstration, please email consumer-nccoe@nist.gov.

CHALLENGE

According to a recent independent analysis, e-commerce fraud increased by 30 percent in 2017, compared to 2016, as malicious actors shift from using stolen credit card data in stores at the checkout counter to using stolen credit card data for fraudulent online shopping. Because online retailers cannot utilize all of the benefits of improved credit card technology, they should consider implementing stronger authentication to reduce the risk of e-commerce fraud.

SOLUTION

This guide explores risk-based scenarios that use multifactor authentication (MFA) to help reduce fraudulent online purchases. In the project's example implementations, if certain risk elements (contextual data related to the transaction) are exceeded that could indicate an increased likelihood of fraudulent activity during the online shopping session, the purchaser will be prompted to present another distinct authentication factor—something the purchaser has—in addition to the username and password.

The NCCoE sought existing technologies that provide the following capabilities:

- integrate MFA into online shopping systems
- mitigate potential exposure to online fraud
- integrate into a variety of retail-information technology architectures
- provide authentication options to retailers:
  - capabilities that assess and mitigate a retailer's shopping-transaction risk factors
  - alert retailer staff to potential threats, and adjust authentication mechanisms as needed

BENEFITS

The NCCoE's practice guide to *Multifactor Authentication for E-Commerce* can help your organization:

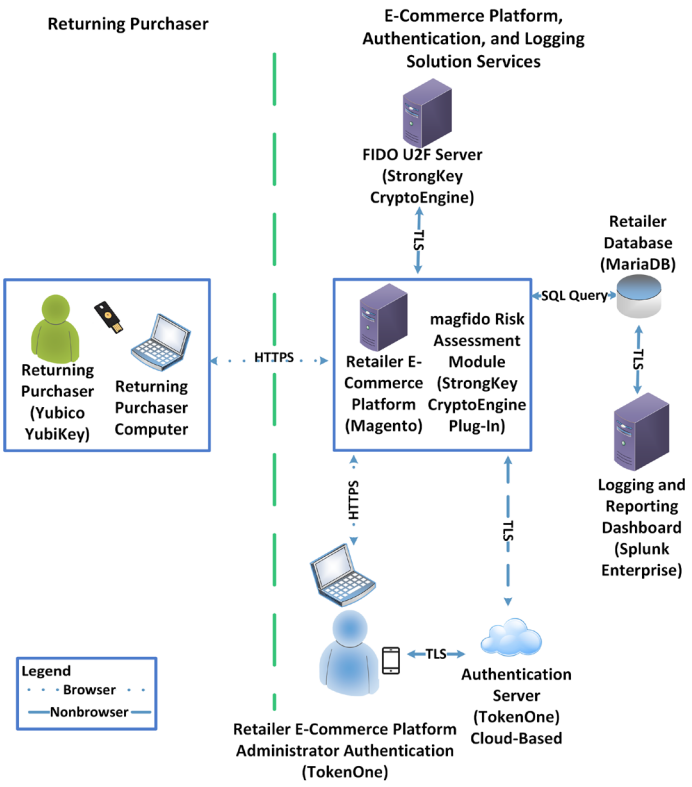
- reduce online fraudulent purchases, including those resulting from the use of credential stuffing to take over accounts
- show customers that the organization is committed to its security
- protect your e-commerce systems
  - provide greater situational awareness
  - avoid system-administrator-account takeover through phishing
- implement the example solutions by using our step-by-step guide

LEARN MORE ABOUT NCCOE
Visit https://www.nccoe.nist.gov

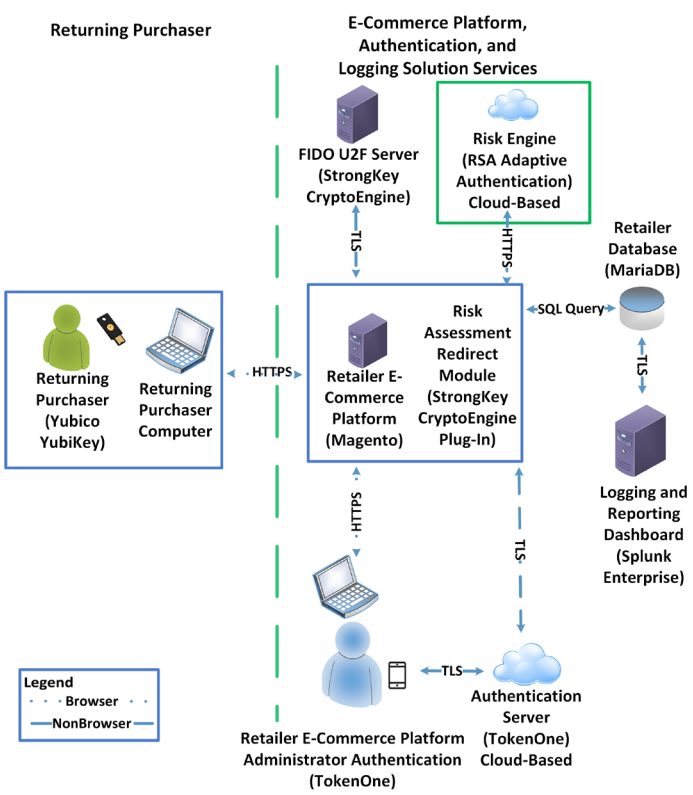
CONTACT US
nccoe@nist.gov
301-975-0200

HIGH-LEVEL ARCHITECTURE

COST THRESHOLD ARCHITECTURE



RISK ENGINE ARCHITECTURE



TECHNOLOGY PARTNERS/COLLABORATORS

The technology vendors who are participating in this project submitted their capabilities in response to a call in the Federal Register. Companies with relevant products were invited to sign a Cooperative Research and Development Agreement with NIST, allowing them to participate in a consortium to build this example solution. Technology collaborators on this project include:

RSA splunk> STRONGKEY TOKENONE yubico

Certain commercial entities, equipment, products, or materials may be identified in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

DOWNLOAD THE PRACTICE GUIDE

For more information about this project, visit: https://www.nccoe.nist.gov/projects/use-cases/multifactor-authentication-ecommerce

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights and expertise from businesses, the public, and technology vendors. If you have feedback on the architecture or the relevance and usefulness of this Practice Guide, or would like to schedule a demonstration, email consumer-nccoe@nist.gov.