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 helping enterprises ensure the security of their online transactions through collaborative efforts with industry and the Information Technology (IT) community, including vendors of cybersecurity solutions. This fact sheet provides an overview of the *Multifactor Authentication for e-Commerce* project description, including background and challenge, goals, and potential benefits. If you would like to propose an alternative architecture or know of products that might be applicable to the challenge of securing e-commerce transactions, please contact us at consumer-nccoe@nist.gov.

BACKGROUND

When chip-and-PIN technology increased security at the point of sale (POS) in the UK and Europe ten years ago, malicious actors turned to e-commerce fraud. As retailers in the United States implement POS security measures, there may be a similar increase in fraudulent, card-not-present (CNP) e-commerce transactions. Consumers, retailers, payment processors, banks, and card issuers are all impacted by fraud. Part of e-commerce fraud reduction includes an increased level of assurance in purchaser or user identity.

CHALLENGE

Retailers recognize that customers could be put off by the complexity that multifactor authentication mechanisms may add to the purchasing checkout and post transaction processes. As such, the NCCoe laboratory build will explore different methods to challenge a consumer to provide multifactor authentication (MFA) when risk calculations and data analytics identify that fraud may be occurring.

GOALS

In collaboration with stakeholders in the retail and e-commerce ecosystem, the NCCoE will demonstrate that implementing risk-based multifactor authentication, tied to existing web analytics and contextual risk calculation, can increase assurance in purchaser or user identity.

This project will explore prompting online customers with additional authentication challenges when web analytics and contextual risk calculations (such as transaction and navigation details, behavioral web session monitoring, and device identification) indicate some doubt that the customer is legitimate. Multiple forms of multifactor authenticators, such as FIDO, out-of-band, and one-time-password devices will be considered to provide retailers and their customers a diverse set of implementation options.

BENEFITS

The potential business benefits explored by this project include:

- reduce risk of fraudulent CNP e-commerce transactions
- increase level of security and assurance for CNP e-commerce transactions
- increase consumer confidence
- receive security alerts from web analytics and risk engine
- automate risk decisions to mitigate risks in real-time
- implement risk based multifactor authentication

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE ABOUT NCCOE
Visit http://nccoe.nist.gov

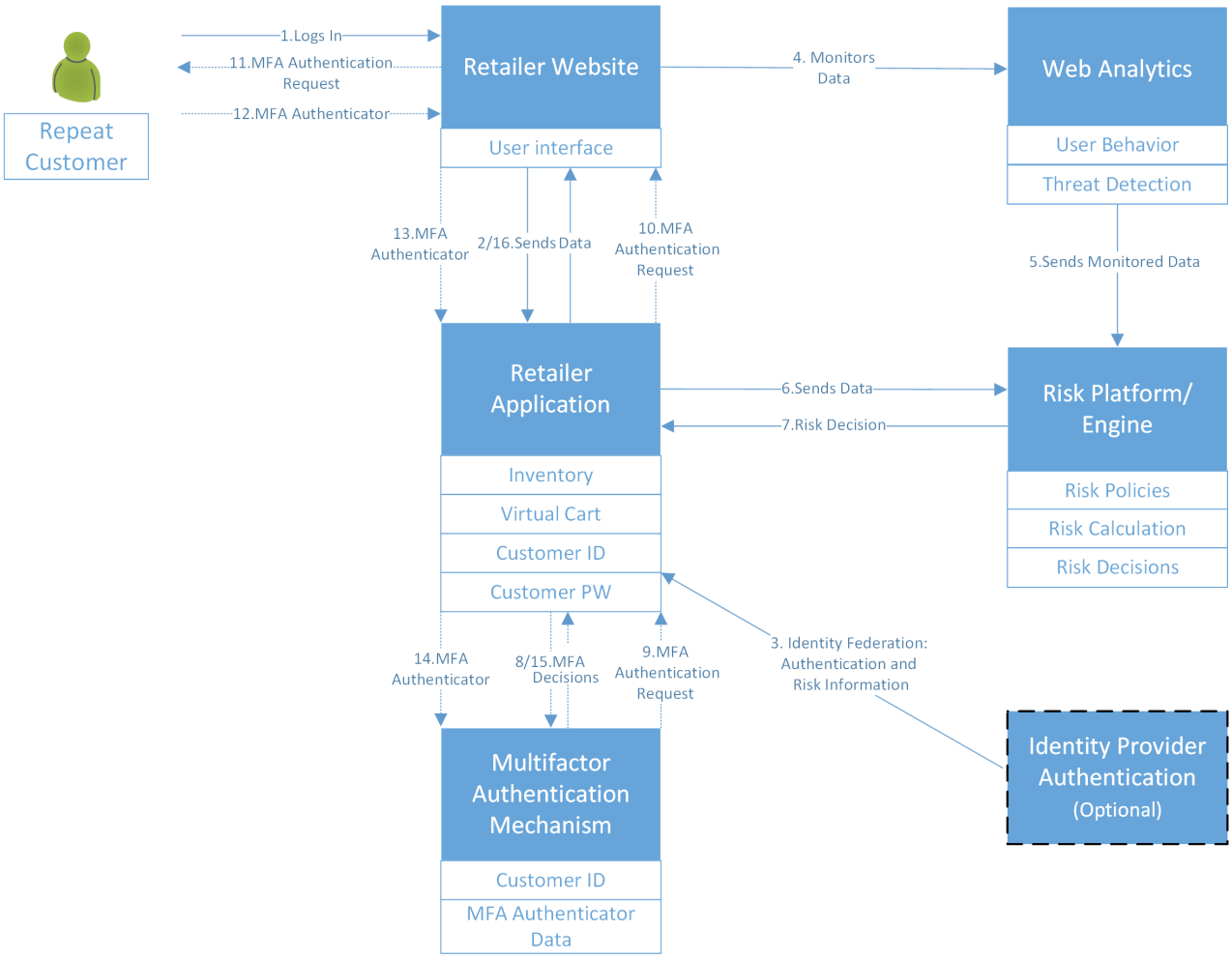
CONTACT US
nccoe@nist.gov
301-975-0200

COMPONENTS

A multifactor authentication solution for e-commerce transactions includes but is not limited to the following components:

- online/e-commerce shopping cart and payment system (in-house or outsourced)
- multifactor authentication mechanisms (types of which will be determined)
- risk calculation platform/engine
- web analytics engine
- logging of risk calculation and web analytics data
- data storage for risk calculation and web analytics data
- identity federation mechanism (optional)

HIGH-LEVEL ARCHITECTURE



TECHNOLOGY PARTNERS/COLLABORATORS

The technology vendors who participated 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:

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 PROJECT DESCRIPTION

For more information about this project, visit: https://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 project, please email consumer-nccoe@nist.gov.