

TLS 1.2 WEBINAR

Everything **SAP Customers** Need to Know

Presented by Steve Park

Monday, September 11, 2017

AGENDA

- + Overview of TLS
- + Customer Impacts
 - + TLS Versions
- + Timeline of Activities
- + Q+A

OVERVIEW OF TLS

What is TLS?

Transport Layer Security

- The TLS protocol provides the key sharing mechanism to encrypt communications between two hosts
- The technology has been around since the 90's and has evolved over time
- SSL became TLS, but the name "SSL" is now a synonym to TLS

SECURE COMMUNICATIONS ARE A MOVING TARGET

Protocol	Availability	Status
SSL 3.0	1996	Insecure
TLS 1.0	1999	Insecure
TLS 1.1	2006	Secure, but limited use
TLS 1.2	2008	Secure
TLS 1.3	2017	In Draft – Not yet released

OVERVIEW OF TLS

Why is CardConnect making changes?

- The [PCI \(Payment Card Industry\) Security Standards Council](#), which defines security and safety rules for the payments industry, no longer considers TLS 1.0 to be a secure form of encryption because it is vulnerable to various types of attacks.
- For additional information on TLS and the risks that are present when using TLS version 1.0, please refer to the PCI Security Standards Council's Information Supplement on [Migrating from SSL and Early TLS](#).

IMPACT TO YOU

How is TLS Used at CardConnect?

- ALL web traffic to cardconnect.com sites are protected with TLS
- CardSecure Tokenizers
- Communications from a merchant's server to CardConnect's APIs
- Any time a client or server passes credentials
- Any time you connect to CardPointe or Copilot

IMPACT TO YOU

Customers impacted by this upgrade include:

Web Browser Support

CardPointe and CoPilot

CardSecure Desktop/Web Tokenizer

CardPointe and CoPilot

CardConnect APIs

SAP

Authorizations / Settlement Calls

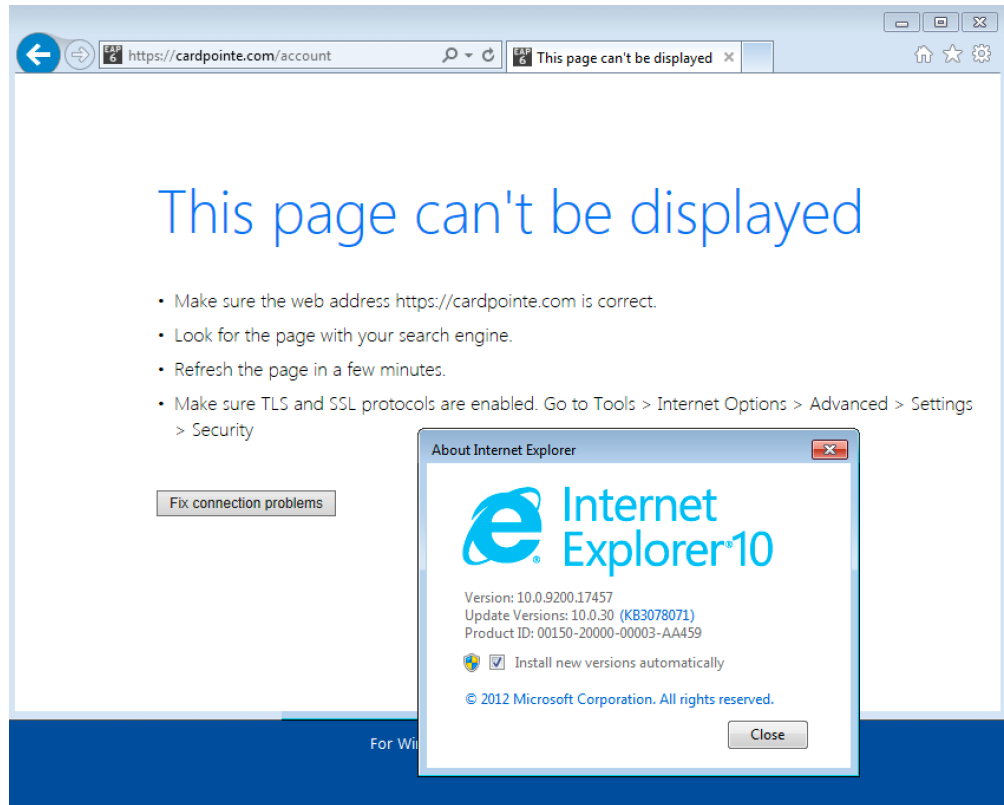
The upgrade to TLS 1.2 could impact you in various ways depending on the manner in which you interact and communicate with CardConnect's applications and systems.

Support Website: <https://support.cardconnect.com/security-resources/tls-1-2-upgrade>

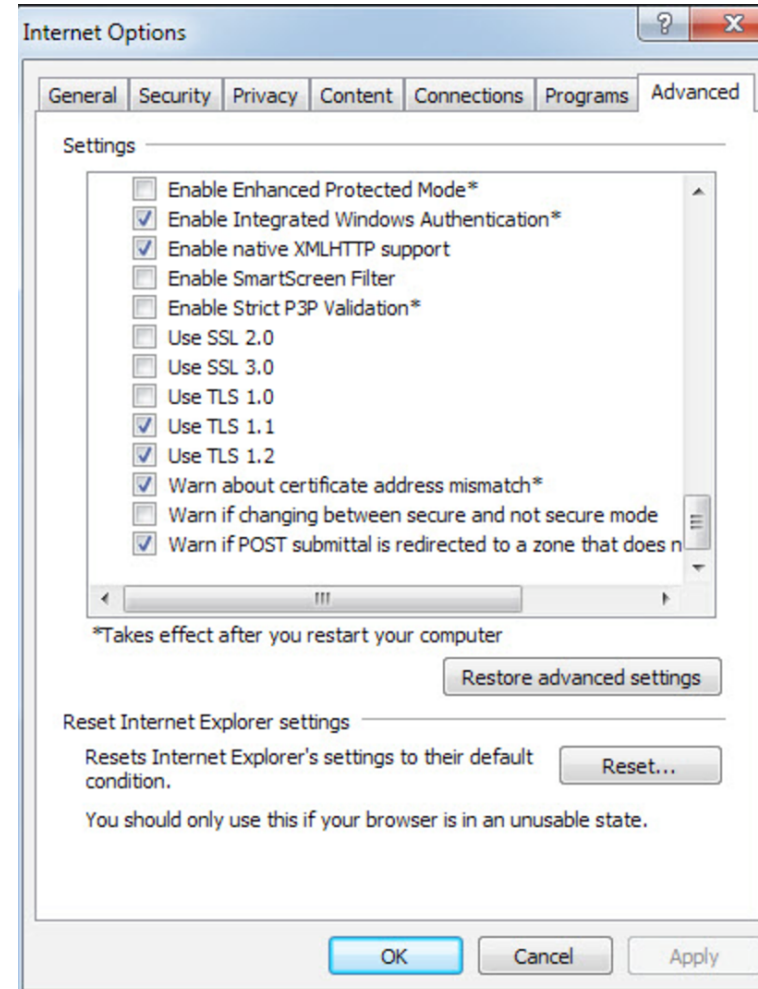
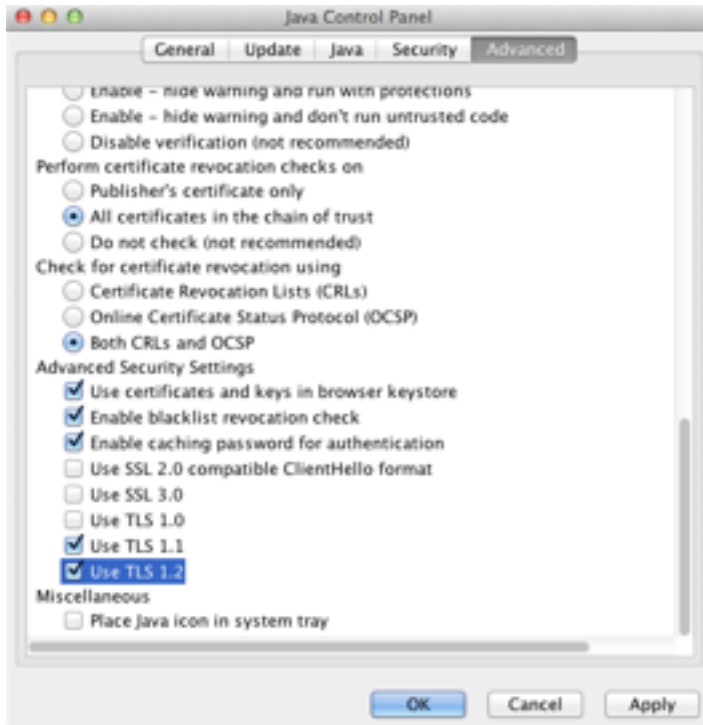
CARDPOINTE + COPILOT TIPS

- Use a modern browser and enable TLS 1.2 if necessary
- Older operating systems (Windows XP) and browsers will received a "handshake failure" message when connecting
- Please refer to the [Web Browser Support](#) section of this page to verify whether your browser(s) is supported by TLS 1.2.
- Support Site: <https://support.cardconnect.com/security-resources/tls-1-2-upgrade#api-gateway-users>

WHAT IS A HANDSHAKE FAILURE?



ENABLE TLS 1.2 WHERE POSSIBLE



API/GATEWAY USERS

- Java Support

- If you run one of the following versions of Java, it is important that you take action before March 31st, 2018 to continue to communicate with CardConnect's services.

Java Version	Details
JDK 7 Client	Yes, but support for TLS 1.2 must be enabled.
JDK 6 and below	No TLS 1.2 support.

- Support Site

- <https://support.cardconnect.com/security-resources/tls-1-2-upgrade#api-gateway-users>

SAP ASSESSMENT TIPS

Three Main ways your SAP systems is connected to CardConnect

1. SAP RFC (TCP/IP) – (Majority of customers)

- SNC enabled – Ensure current SAPCryptolib
- SNC not enabled
 - Currently you will not have to update anything in your SAP system at this point.
 - Future planning for upgrading to JSON Rest API via HTTPS. For those interested to transition early please contact ERPSupport@cardconnect.com

2. SAP RFC (HTTP connection to External Server)

Ensure current SAPCryptolib

3. SAP PI –

Ensure current Java Cryptolib

SAP RFC (TCP/IP) + SAP HTTPS CALL FROM SAP

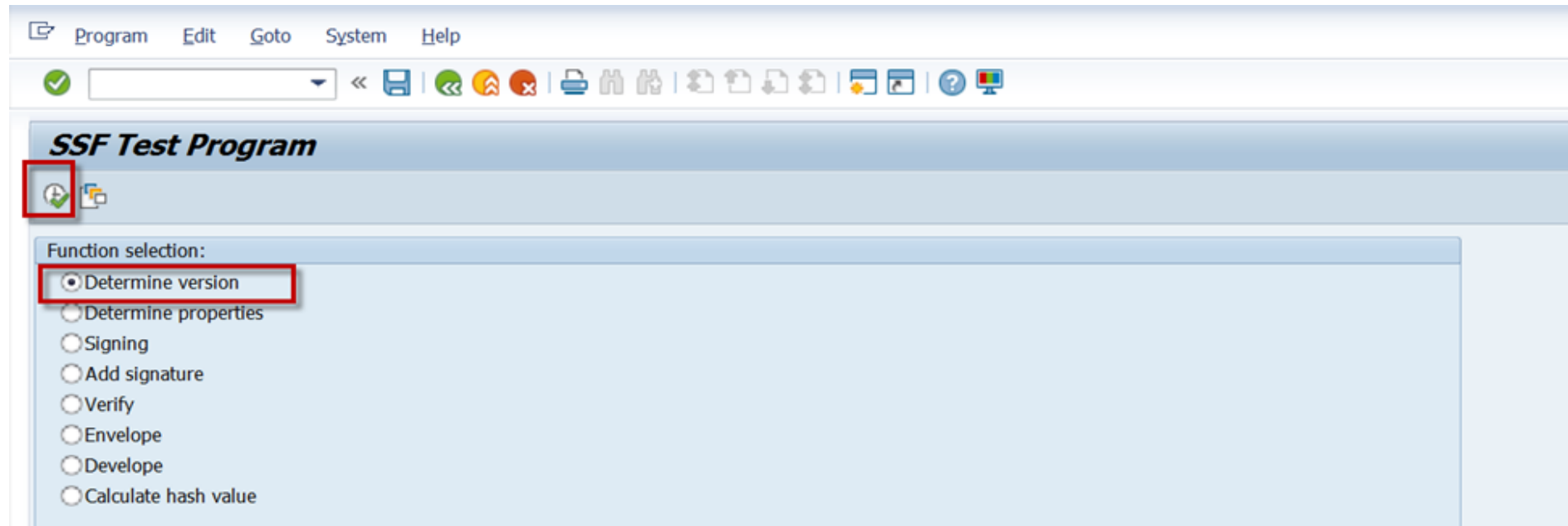
What version of the SAP Crypto Library is needed?

Minimum Cypolib is **8.4.31**

How to determine the current SAP Crypto Library

- Standard SAP Program: **SSF02**
- Run the program with the default values
 - Just ensure that the 'Determine version' radio button is selected*

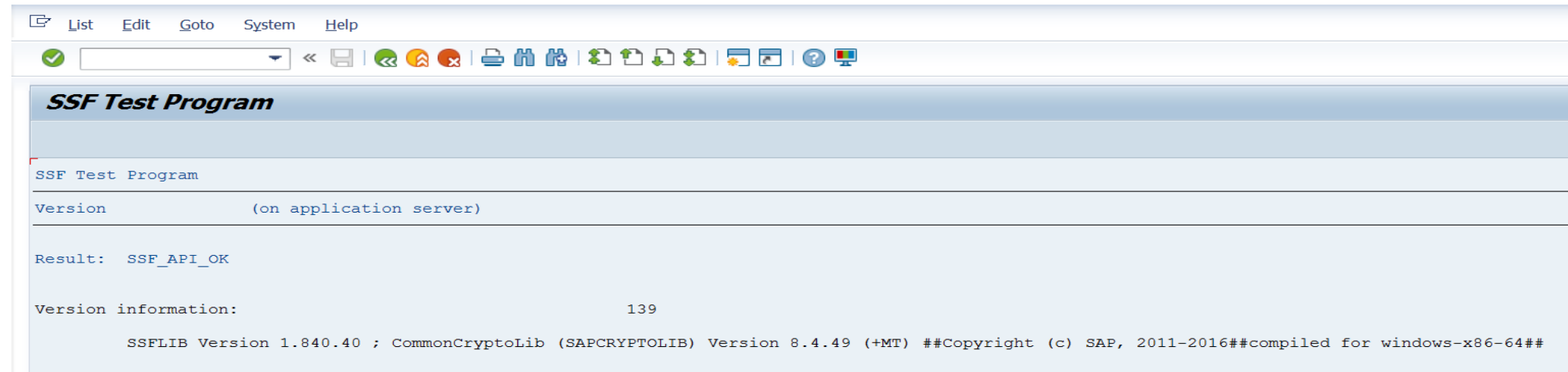
SAP RFC (TCP/IP) + SAP HTTPS CALL FROM SAP



SSF02

SAP RFC (TCP/IP) + SAP HTTPS CALL FROM SAP

- Results of the execution of the program
- Minimum SAPCRPTOLIB is **8.4.31**



The screenshot shows the SAP command line interface. At the top, there is a menu bar with 'List', 'Edit', 'Goto', 'System', and 'Help'. Below the menu bar is a toolbar with various icons. The main area displays the following text:

```
SSF Test Program  
  
SSF Test Program  
-----  
Version                (on application server)  
-----  
Result:  SSF_API_OK  
  
Version information:                139  
SSFLIB Version 1.840.40 ; CommonCryptoLib (SAPCRYPTOLIB) Version 8.4.49 (+MT) ##Copyright (c) SAP, 2011-2016##compiled for windows-x86-64##
```

Internal SAP System: 8.4.49

SAP RFC (TCP/IP) + SAP HTTPS CALL FROM SAP

Importing a new CommonCryptoLib (SAPCRYPTOLIB)

OSS note **1848999** - Central Note for CommonCryptoLib 8 (SAPCRYPTOLIB)

- This note provide the detail on the latest Crypto Library
- Reference **OSS note 510007**

This note will describe the default cipher suite priority to be used

SAP PI

Uses SAP Java Cryptographic Toolkit (a.k.a. IAIK)

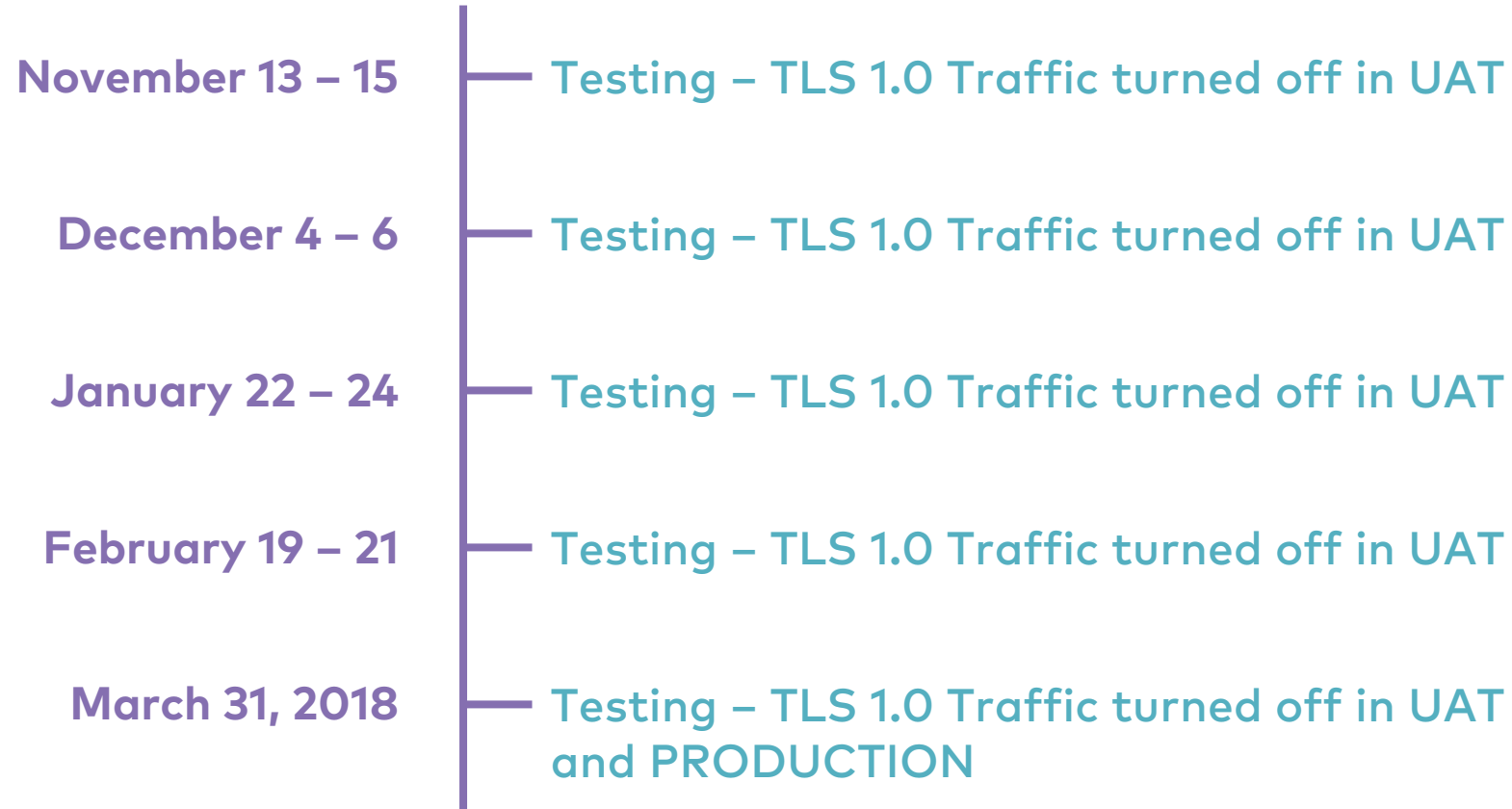
OSS Note: 2284059 - Update of SSL library within NW Java server

- This note describe the new IAIK library that now supports TLS 1.2.

Excellent PI Blog to describe an upgrade to TLS 1.2

<https://blogs.sap.com/2017/06/09/chronicles-of-a-tls-1.2-upgrade/>

TIMELINE OF TESTING ACTIVITIES





Q + A

A person wearing a striped shirt is holding a white coffee cup with a black lid in their left hand and a card in their right hand. The background is blurred, showing a person in a white shirt. The CardConnect logo is overlaid in the center.

cardconnect[®]
A First Data Company