



# **V1 BACS 6.3 Release Overview (External)**

Julie Edwards, Senior Product Manager  
February 2018

# General Disclaimer

*This document is not to be construed as a promise by any participating company to develop, deliver, or market a product. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. V1 Ltd makes no representations or warranties with respect to the contents of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. The development, release, and timing of features or functionality described for V1's products remain at the sole discretion of V1 Ltd. Further, V1 Ltd reserves the right to revise this document and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.*

# Content

## 1. Market Update

- ▶ Mandated changes – Internet Security
- ▶ BACS Cyber Security Programme

## 2. Release 6.3

## 3. Useful Information



## Background

# Market Update - Mandated Changes

## Changes Driven by the Internet Community

The internet community is **adopting a more sophisticated level of internet security** – a move away from SHA-1 SSL certificates to SHA-2 SSL certificates

SHA-2 (or SHA 256 to give it its full name) is an improved means of protecting secure internet sites. It stands for Secure Hash Algorithm, and was designed by the National Institute of Standards and Technology (NIST). It is being adopted by all internet providers from 1 January 2017

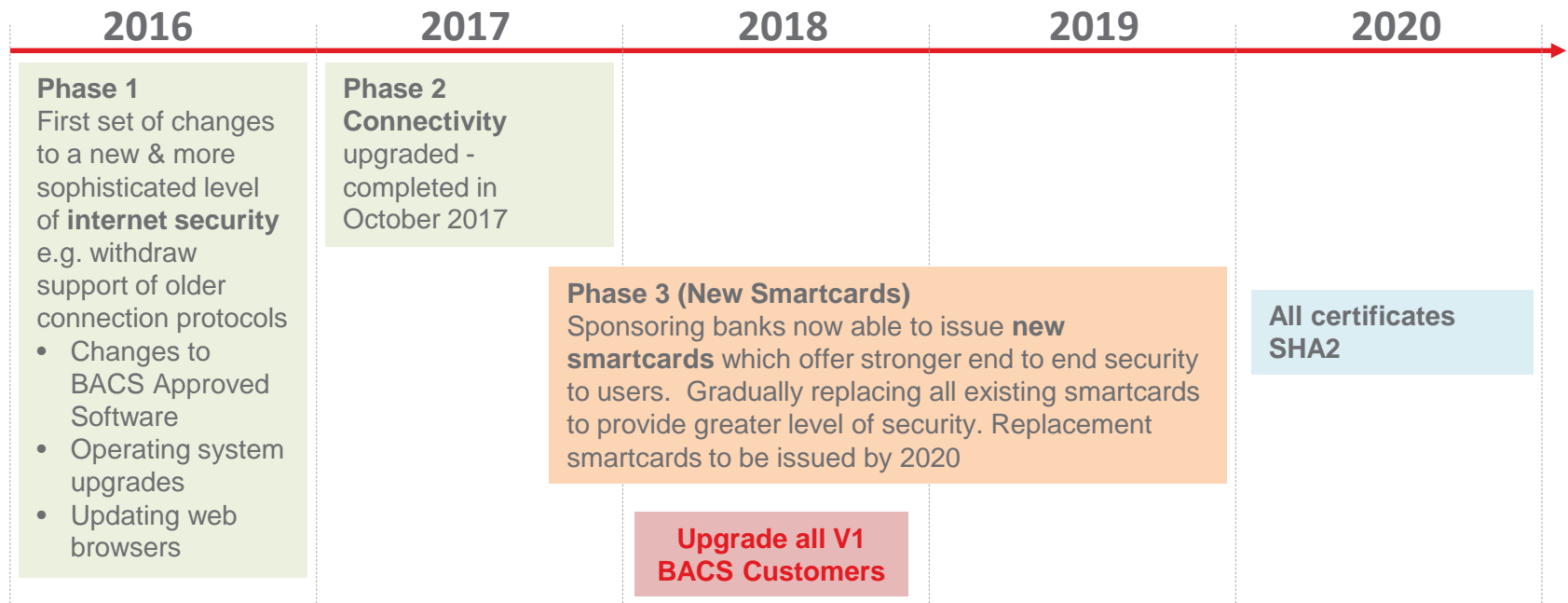
## Changes Driven by the Payments Industry

At the same time as the internet community moves to the new SHA-2 certification, BACS are **withdrawing support for older connection protocols** to provide even more protection for the communications pipeline between the Payment Services Website (PSW), and service users.

BACS now only support TLS 1.1 and 1.2.

# BACS Cyber Security Programme

Multi-phase enhanced cyber security programme – partly driven by the internet community (a move SHA-2 SSL certificates); partly driven by BACS (withdrawing support of old connection protocols)



## Phase 3 – New Smartcards

- ▶ Authentication with BACS (logging in or signing a submission) uses a smartcard containing a certificate
  - ▶ Currently uses a cryptographic method called **SHA1** to provide security
- ▶ BACS (& the wider banking community) are in the process of transitioning to the use of the cryptographically stronger **SHA256** method
  - ▶ This involves issuing new smartcards to users and making changes to software (such as V1 BACS)
  - ▶ During this transition period, BACS will accept both SHA1 and SHA256 authentication
  - ▶ At the end of this period (anticipated to be during 2019, possibly sooner), SHA1 authentication will no longer be accepted



**Release 6.3**



# Release Overview

- ▶ V1 BACS R6.3 provides **full support for SHA-256 certificates & smartcards** and includes a number of **technology modernisation** enhancements.
- ▶ It replaces the current version (6.0.1.xxxx) and older versions
- ▶ Existing DbBACS customers must upgrade to R6.3 i.e. this is a **mandatory upgrade**.
- ▶ If you do not upgrade, you will be unable to make BACS submissions once SHA1 support is removed
- ▶ BACS & Vocalink are encouraging customers to upgrade by the end of 2018

# Release Snapshot

## Value Add Capability

- ▶ Fully SHA256 compliant
    - ▶ SHA256 authentication with new smart cards
    - ▶ Fall-back SHA1 authentication when used with older smart cards
  - ▶ Seamless solution during the transition period
  - ▶ [BACS Approved Software Solution \(BASS\)](#)
- 

## Issues Resolved

- ▶ Better handling of Bureaux Service User Numbers
  - ▶ Secure Session indicator shows as soon as BACS connection is established
  - ▶ Improved clarity in error messages
  - ▶ Stricter handling of Direct Debit Instruction submissions
  - ▶ Minor changes to track compliance requirements
- 

## Compliance & Legislation

- ▶ A mandatory change driven by the internet community to improve internet security; mandated by BACS and the wider banking community
- ▶ Supported platform changes: n/a



## Useful Information

# Upgrading to 6.3

- ▶ Upgrading is mandatory (strongly recommended by end of 2018)
- ▶ Software available free of charge (with active S&M)
- ▶ Services chargeable – estimated ½ day remote upgrade per customer

# Supported Versions – Reminder

- ▶ Standard supported versions policy
  - ▶ “Support & maintain the current major release version of each product plus the previous major release”
  
- ▶ V1 BACS will be an exception:
  - ▶ From December 31 2018, we plan to cease support & maintenance for all DbBACS versions before R6.3
  
- ▶ From 1<sup>st</sup> January 2019, V1 BACS Release 6.3 (onwards) will be the only version we support and maintain

# Summary

## 6.3

Provides full support for SHA-256 certificates & smart cards & includes a number of technology modernisation enhancements.

Replaces current version 6.01.xxxx and all previous/older versions

All existing customers **must** upgrade by the end of 2018 to ensure uninterrupted BACS submissions

**Available: March 7 2018**



Please contact your Account Manager  
to arrange your upgrade