THALES
Building a future we can all trust

payShield: Compliance, Certification & Cloud

JAMES TORJUSSEN
Payments Product Management

www.thalesgroup.com

James Torjussen

Payments Product Management

Table of contents

01 Market Drivers & Influencers

02 Roadmaps

03 Certification

04 PQC Update

05 payShield Cloud HSM

06 Managed Services

07 Prime Factors' BCSS

08 Useful Links

Market Drivers & Influencers

Australian Payments Network Connect Inspire Thrive

PCI Security Standards Council®

AMERICAN EXPRESS

NIST

FIPS VALIDATED 140-2

Bancontact

girocard

UnionPay 银联

CB

ANSI American National Standards Institute

BANCOMAT

eftpos

DISCOVER NETWORK

JCB

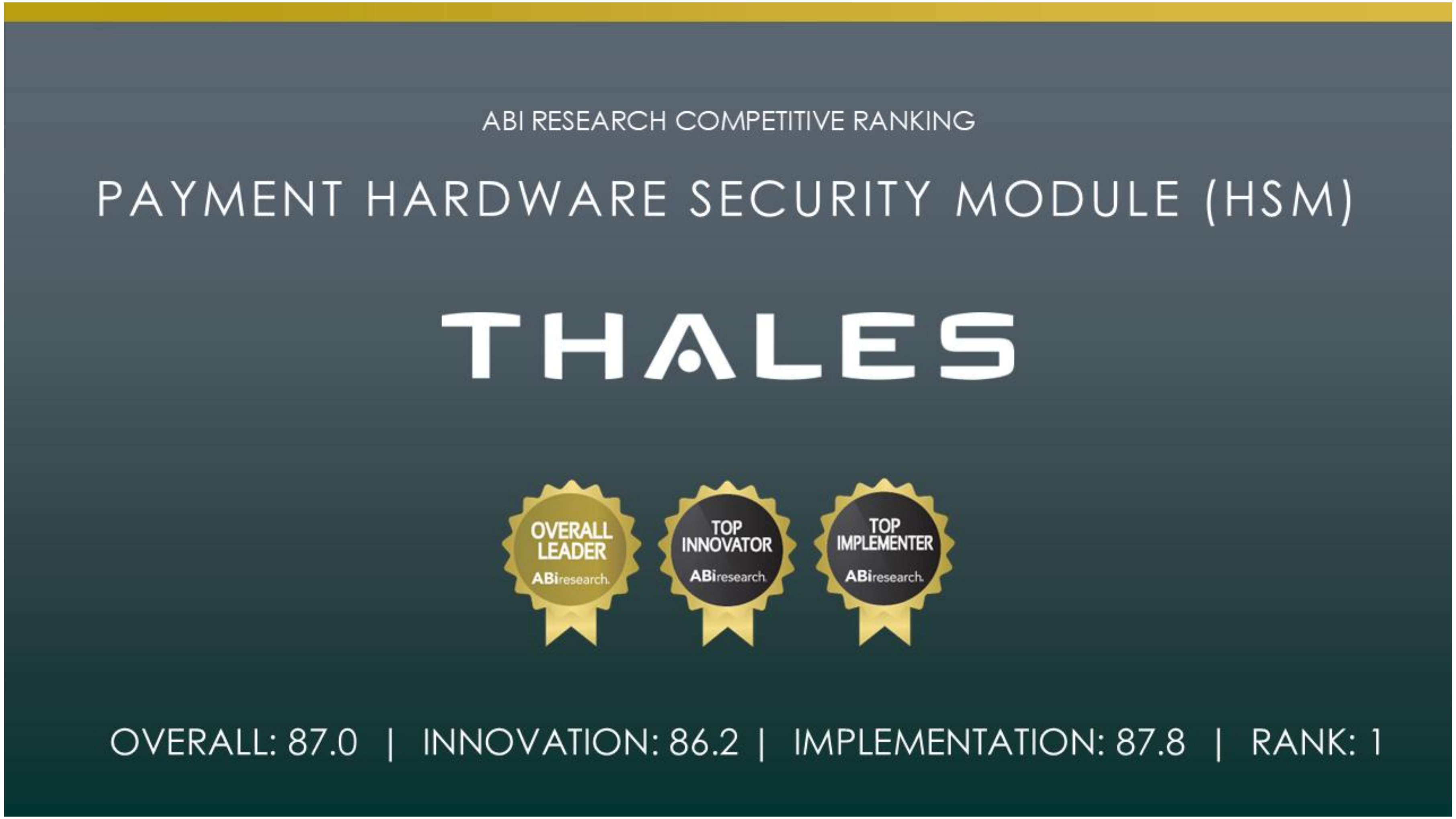
mastercard

VISA

ISO International Organization for Standardization

EMVCo™

GLOBALPLATFORM



ABI RESEARCH COMPETITIVE RANKING

PAYMENT HARDWARE SECURITY MODULE (HSM)

THALES

OVERALL: 87.0 | INNOVATION: 86.2 | IMPLEMENTATION: 87.8 | RANK: 1

payShield 10K Roadmap

Planned releases

v2.2a – v2.2b – released July 2025

TR-34 – Import Key under RSA

TR-34 - Export Key under ECC (Verifone VRK2)

PIN Translation - TPK to AES DUKPT & GBIC

v2.3a – due now

CVV, dCVV & iCVV support using AES

v2.4a – planned Q4/2025

TLS v1.3, PAN translation with authentication

v2.5a – planned Q2/2026

TLS certificate renewal – automation

Backlog features

API enhancements

AES Limited Use Keys (LUK) for cloud payments

AES GCM & CCM encryption modes

AES key padding in key blocks

ECC Brainpool curves

EC-SDSA (Schnorr) signature generation/verification

X9.143/TR-31/ISO 20038 key block enhancements

X9.139/TR-34 updates

AusPayNet key block support

payShield Monitor & TMD Roadmap

Planned releases

payShield Monitor v3.0.0 – estimated mid 2025

Migration of base operating system

payShield TMD v2.16 – released June 2025

HMAC key component generation

payShield TMD Hardware Refresh – est early 2026

New TMD hardware model – PCI HSM KLD v4 approved

Backlog features

payShield Monitor

View security configuration

View settings per LMK

Download error and audit logs

payShield TMD

Maintenance releases

payShield 10K Roadmap

Certifications

PCI HSM v3 (expires 30th April 2026)

v2.0c, v2.1a, v2.2b – approved

v2.3a – preparing for evaluation

PCI HSM v4 (expires 30th April 2032)

Submitted for approval

Certificate expected Q4 / 2025

FIPS 140-3 Level 3

Preparing for evaluation

Regional Certifications

France - SAFIRE 2.2 (CB-HSM)

Custom software (v1.5a) – approved

France - SAFIRE 2.3 (CB-HSM)

v2.0c – submitted for approval

Custom software (v2.0c) – preparing for evaluation

Germany - GBIC

v1.7b, v1.9b, v1.9c, v2.2a – approved

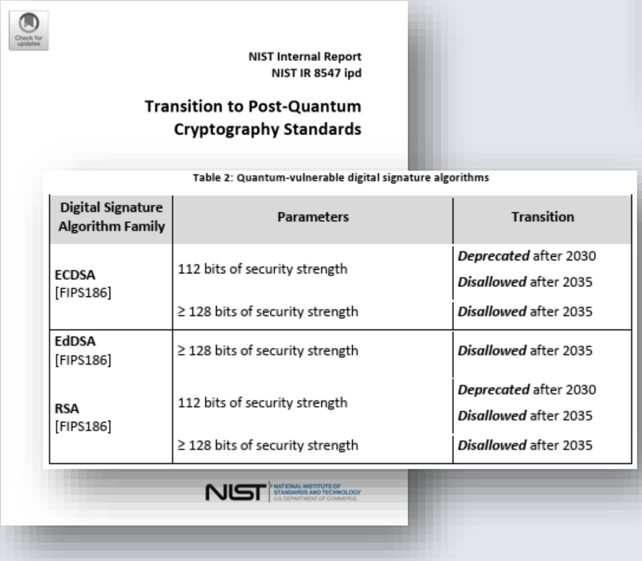
Belgium - Bancontact

Listed on the Bancontact website since March 2022

AusPayNet

1.9a, 1.9b, 1.9c, 1.9d, 2.0c – approved

PQC Update – card/mobile transactions



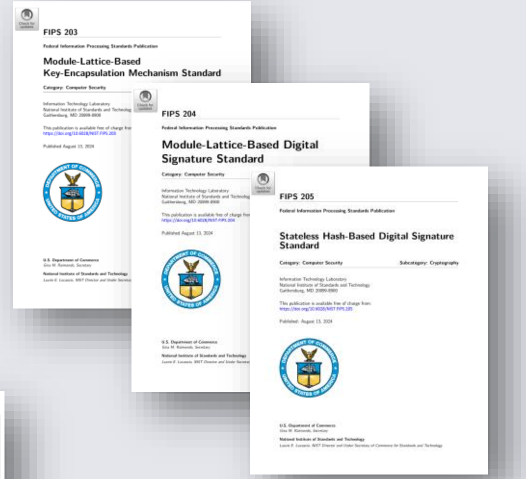
NIST Internal Report
NIST IR 8547 ipd

Transition to Post-Quantum Cryptography Standards

Table 2: Quantum-vulnerable digital signature algorithms

Digital Signature Algorithm Family	Parameters	Transition
ECDSA [FIPS186]	112 bits of security strength	*Deprecated* after 2030 *Disallowed* after 2035
	≥ 128 bits of security strength	*Disallowed* after 2035
EdDSA [FIPS186]	≥ 128 bits of security strength	*Disallowed* after 2035
RSA [FIPS186]	112 bits of security strength	*Deprecated* after 2030 *Disallowed* after 2035
	≥ 128 bits of security strength	*Disallowed* after 2035

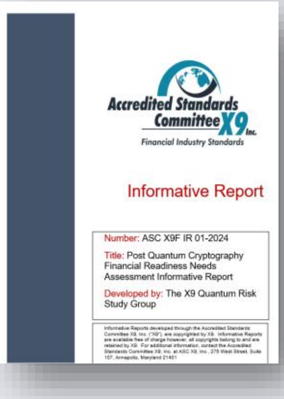
NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE



FIPS 203
Federal Information Processing Standards Publication
Module-Lattice-Based Key-Encapsulation Mechanism Standard
Category: Computer Security
Information Technology Laboratory
National Institute of Standards and Technolog
Gaithersburg, MD 20899-8900
This publication is available free of charge fro
https://doi.org/10.6028/NIST.FIPS.203
Published August 13, 2024
U.S. Department of Commerce
Gina M. Raimondo, Secretary
National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary

FIPS 204
Federal Information Processing Standards Publication
Module-Lattice-Based Digital Signature Standard
Category: Computer Security
Information Technology Laboratory
National Institute of Standards and Technolog
Gaithersburg, MD 20899-8900
This publication is available free of charge fro
https://doi.org/10.6028/NIST.FIPS.204
Published August 13, 2024
U.S. Department of Commerce
Gina M. Raimondo, Secretary
National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary

FIPS 205
Federal Information Processing Standards Publication
Stateless Hash-Based Digital Signature Standard
Category: Computer Security Subcategory: Cryptography
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900
This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.205
Published: August 13, 2024
U.S. Department of Commerce
Gina M. Raimondo, Secretary
National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology



Accredited Standards Committee X9 Inc.
Financial Industry Standards

Informative Report

Number: ASC X9F IR 01-2024
Title: Post Quantum Cryptography Financial Readiness Needs Assessment Informative Report
Developed by: The X9 Quantum Risk Study Group

Informative Reports developed through the Accredited Standards Committee X9, Inc. ("X9"), are copyrighted by X9. Informative Reports are available free of charge however, all copyrights belong to and are retained by X9. For additional information, contact the Accredited Standards Committee X9, Inc. at ASC X9, Inc., 275 West Street, Suite 107, Annapolis, Maryland 21401

PCI Security Standards Council

Payment Card Industry (PCI)
PIN Transaction Security (PTS)
Hardware Security Module (HSM)

Modular Security Requirements
Version 5.0
June 2024

DRAFT

Online EMV cryptograms use symmetric keys

AES-256 is resistant to quantum attacks

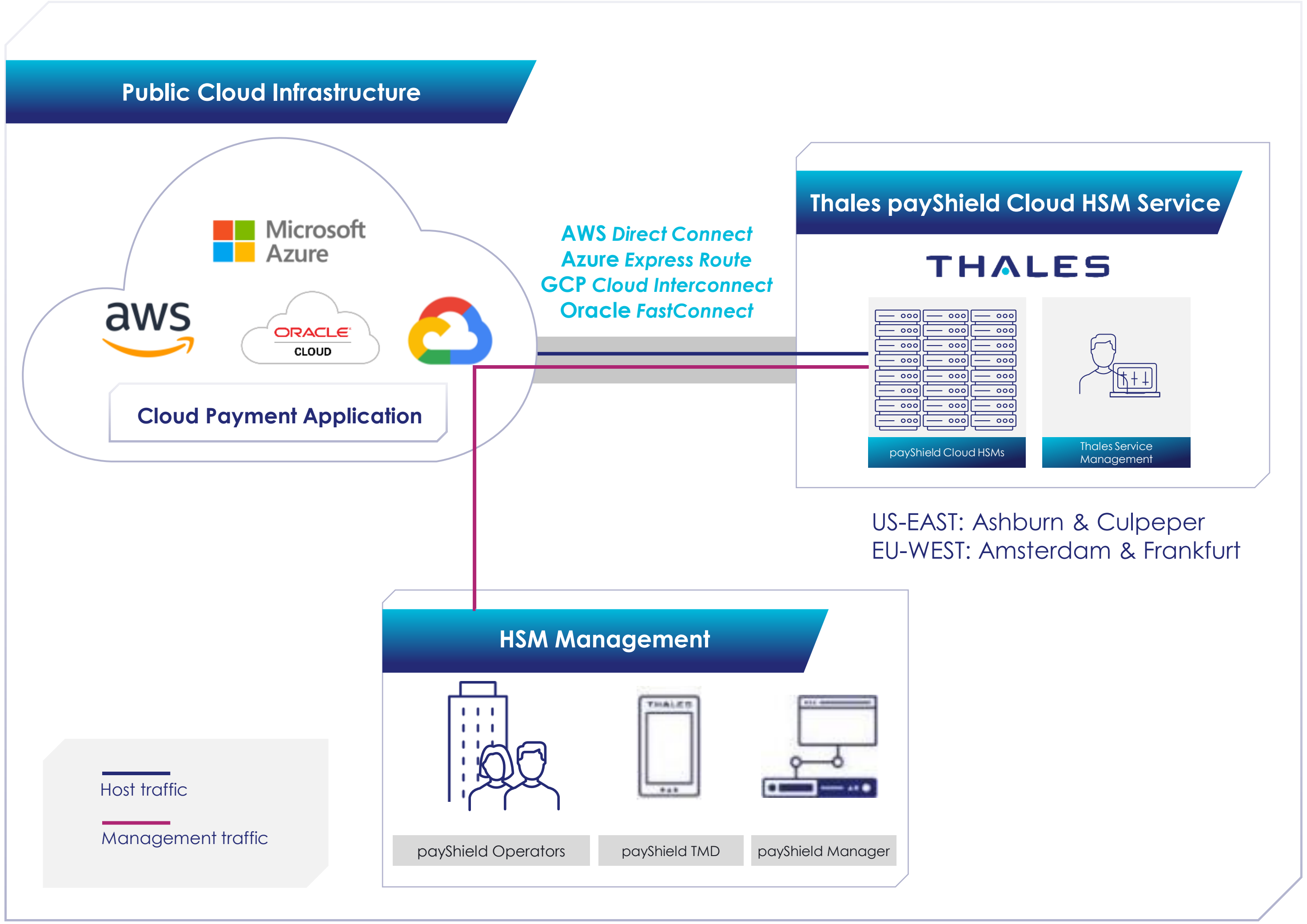
Offline EMV cryptograms use asymmetric keys

But no threat from "harvest now, decrypt later"

But..

Remote key loading, mobile payments, other schemes

payShield Cloud HSM



Public Cloud Infrastructure

Cloud Payment Application

AWS Direct Connect
Azure Express Route
GCP Cloud Interconnect
Oracle FastConnect

Thales payShield Cloud HSM Service

payShield Cloud HSMs

Thales Service Management

US-EAST: Ashburn & Culpeper
EU-WEST: Amsterdam & Frankfurt

HSM Management

payShield Operators

payShield TMD

payShield Manager

Host traffic

Management traffic

HSMs hosted in **secure Thales data centers**

Proven integration with **all major public clouds**

Access to HSMs via a **flexible subscription service**

Low latency, **high performance** connections

Full **remote management** of HSMs

payShield Cloud HSM

New enhancements

Improved SLA

DPoD Tile Marketplace

Free 30-day trial service

VPN access

Managed Services via Partners – e.g. A24

Thales advantages

Dedicated cage with multiple cabinets

Redundant network infrastructure

Connection via Equinix fabric, VPN, etc.

Dual control access to cage & cabinets

Continuous CCTV monitoring inside cages

Competitive Analysis

Microsoft - Azure Payment HSM
Must spend $$$ in Azure compute

Utimaco – MYHSM
Shared HSM / Dedicated HSM

Owned by competitor / Questionable long-term availability

Amazon - AWS Payment Cryptography API
Lacking some essential functionality

Incompatible with third party applications

Use cases

Test

DR

Production

Managed Services

Complements our existing “bare-metal” hosted HSM offering to save time and reduce risks

- Specialist resources
- Key management
- Networking & security
- Migration to cloud
- Compliance

A24 THALES Building a future we can all trust

Managed Services from A24 Optimised for payShield Cloud HSM

EXPERT ASSISTANCE SAVING YOU TIME AND REDUCING YOUR RISK

High Level API

Prime Factors - Bank Card Security System (BCSS)

Accelerates development of new payment applications

Provides a high-level API rather than the “legacy” low-level payShield API

Contains building blocks such as load balancing, HSM drivers, diagnostics

Includes key management functionality for payment issuing / processing

Helps customers meet PCI requirements via audit reports & compliance checklists

Prime Factors Bank Card Security System (BCSS) powered by Thales payShield 10K

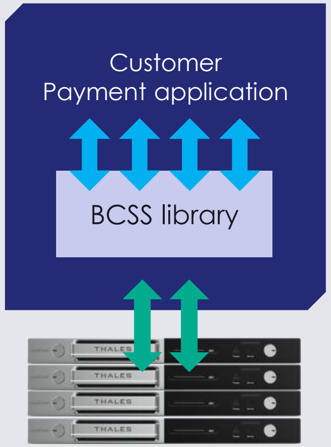
Get payment system development costs under control with Prime Factors and Thales

Simplifying payments security

Solution Brief

Building More Secure Payment Applications Faster

Leveraging Prime Factors Bank Card Security System and Thales payShield for Better Security, Efficiency, and Agility



Payment security is complex. It takes special knowledge, skills, and even language to understand, implement, and maintain. BCSS simplifies all of this, which helps **close sales quicker and easier**, at a higher price point for resellers, while saving your customers money and locking out competition, since BCSS only supports the Thales payShield.

Useful Links

payShield 10K

Datasheet

Product Brief

Transaction Processing using payShield HSMs

Payment Credential Issuing using payShield HSMs

Top 10 Reasons for migrating

ABI research's Payment HSM Competitive Ranking

payShield TMD

Datasheet

Product Brief

Top 10 Reasons for using

payShield Monitor

Datasheet

Product Brief

payShield Cloud HSM

Business Brief

Technical Brief

Brochure

Top 10 Reasons

Customer Presentation

Managed Services from A24

BCSS

Building More Secure Payment Applications Faster

Solution Brief

THALES

Building a future we can all trust

Thank you

www.thalesgroup.com