HITACHI
Inspire the Next

HITACHI BIOMETRIC SOLUTIONS FOR RETAIL BANKING

Hitachi's digital security portfolio includes a comprehensive biometric solution for retail banking.

Hitachi Digital Security

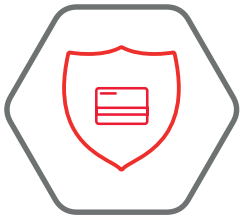
BASED ON HARDWARE, SOFTWARE AND RELATED SERVICES, BANKS ARE ABLE TO DEPLOY VeinID TECHNOLOGY TO DRIVE OPERATIONAL IMPROVEMENTS, INCREASE EFFICIENCY AND CONTRIBUTE SIGNIFICANTLY TO DIGITAL SECURITY.

USING THE UNIQUE PATTERNS OF BLOOD VESSELS INSIDE THE FINGER FOR THE AUTHENTICATION AND VERIFICATION OF IDENTITY OF BOTH CUSTOMER AND STAFF, VeinID IS A SECURE, SIMPLE TO USE AND EXTREMELY FAST AND EFFICIENT SOLUTION FOR USE IN A VARIETY OF MARKET SECTORS.

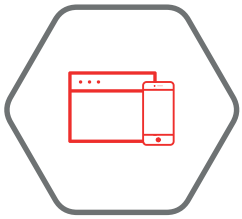
HITACHI
Inspire the Next

Hitachi Digital Security

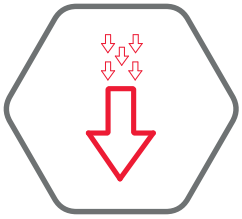
BENEFITS



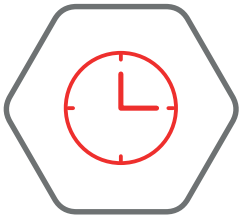
Increase the level of security of transactions via strong authentication – peace of mind for customers and improved controls within the bank.



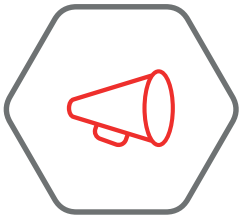
Offer a better transaction package to customers based on a more secure process.



Simplify the customer experience, speed up the time taken to process transactions, no need to remember PIN codes, new possibilities for card-less transactions.



Improvement of the internal processes within the bank – reach digitalisation targets, reduce the costs and complexities of paper handling, free up time for staff to consult with customers and drive sales.



Promotion of the bank as an innovative and modern institution.

VeinID HAS BEEN SUCCESSFULLY USED TO AUTHENTICATE TRANSACTIONS AT AUTOMATED TELLER MACHINES (ATMS) AND IS COMPATIBLE WITH MACHINES FROM THE MAIN MANUFACTURERS INCLUDING WINCOR NIXDORF, NCR AND DIEBOLD.

Based on biometric authentication, users can make secure cash withdrawals, deposits and other local transactions such as withdrawals of social benefits and pensions, without using cards or PIN codes.

VeinID can also be used as an additional security feature for traditional card and PIN based EMV transactions. Encrypted biometric templates are stored safely inside the bank's secure environment in a central server or on a suitable smart card.

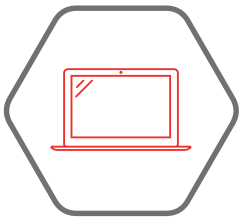
BIOMETRIC BRANCHES

The use of VeinID in a bank branch allows for both the verification of customer's identity and for the authorisation of transactions. Opening new accounts, withdrawal of savings, transfers between accounts, and the signing of various types of agreements can all be protected using VeinID solutions. Biometric templates are stored on a secure bank server or on a smart card.

AUTHENTICATING DIGITAL SIGNATURES (BIOMETRIC PKI)

VeinID BioPKI is used instead of traditional smart card and PIN codes for authenticating digital signatures. It is compatible with Public Key Infrastructure (PKI) platforms and provides back office certificate management, key storage and signature creation processes. It allows for digital signing without using smart cards, PINs or passwords and can be used for authenticating both the bank's staff and customers in all transactions where digital signatures are needed.

Used to replace the handwritten signature of the customer, it can validate loan agreements, bank transfers, account opening etc. A key tool for enabling paperless operations, it reduces costs of paper document processing and plays a central role in helping to deliver the bank's digital transformation agenda.



MOBILE ADVISOR

Used with a laptop PC, this solution allows the bank to extend the services on offer in the traditional branch environment to all customers who are either acquired or serviced outside of the normal bank branch.

INTERNAL SECURITY

Significantly increase internal security and control access to critical information. VeinID solutions can protect workstations from unauthorised access, provide secure domain logon, integrate with Single Sign On systems and can be used to manage transaction level authentication of bank staff. When used with physical access control systems, it can guarantee the safety of strategic resources that need special protection such as server rooms, secure offices, safety deposit boxes etc.

FINGER VEIN SERVER (FVS) IS A CENTRAL SYSTEM FOR MANAGING ALL ASPECTS OF VeinID PROCESSING AND IS RESPONSIBLE FOR:

- The security of transactions and related audit trails and reporting.
- The registration and authentication of customers and staff.
- The servicing, monitoring and management of biometric readers including security key management.

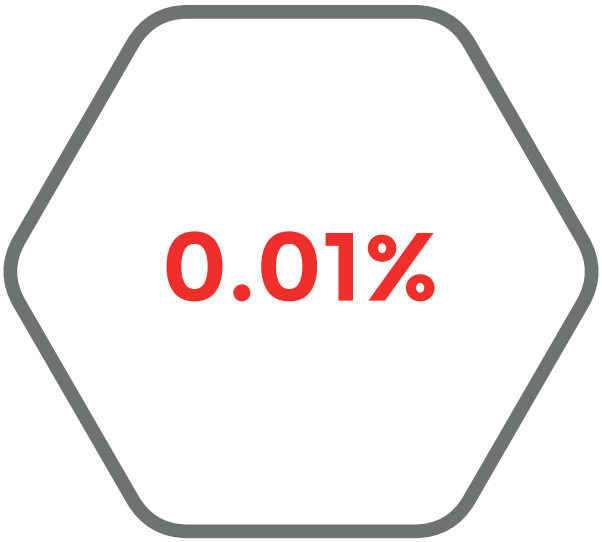
FVS can be integrated with banking systems via Web Services Application Programming Interfaces (APIs) and supports authentication of self-service and over-the-counter transactions. There are client components for installation onto ATMs, Virtual Teller Machines (VTMs), bank branches, information kiosks and web applications. Biometric templates are stored securely in an encrypted database and optional modules for VeinID monitor and content management can be added. It supports connections from VeinID devices inside the bank's secure network as well as connections via the internet (via a special Finger Vein Proxy Server).

VeinID BioPKI SERVER

BioPKI is an optional module to manage: authentication of digital signatures by VeinID, creation of digital signatures via a hardware security module and attaching of digital signatures to agreement documents (e.g. pdf or word files) created by the bank's systems. It includes a certificate authority to manage the issuing and lifecycle of digital certificates along with optional time stamp server and log management tools. Private keys for customers and staff are created securely inside an Hardware Security Module (HSM) during the registration process, encrypted under the HSM master keys and then stored in encrypted form inside the BioPKI database. After a successful authentication of a customer via VeinID, a digital signature is created inside the HSM via secure code execution and attached to the agreement. The document is passed to the bank's systems for further processing.

Scanned biometric data, depending on the bank's policies, can be stored on the central server and on a suitable smart card/secure token if needed. Live-scan biometric templates from customers are matched on a secured reader.

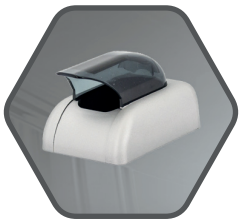
False acceptance rate.
The proportion of verification transactions with wrongful claims of identity that are incorrectly confirmed.



False rejection rate.
The proportion of verification transactions with truthful claims of identity that are incorrectly denied.

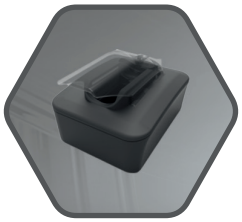
FVID BRANCH READER

Based on the HOTS 609UE, it is dedicated to over the counter use by staff or customers in the bank branch. Used for customer and staff registration and authentication, authentication of teller transactions or for customer service. Available with either USB or Ethernet interfaces, the Ethernet version acts as a network appliance and includes a dedicated micro-switch for plug and play connectivity. Designed to be used inside the bank's secure network.



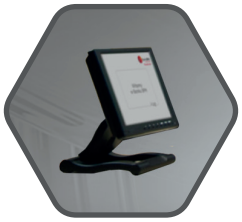
FVID ATM READER

Based on the HOTS 609UE module and designed for assembly onto an ATM or other banking self-service device such as VTM or information kiosk, it provides authentication of transactions and operations such as cash withdrawal or social benefits payments. It can be installed on devices operating both indoors or outdoors. Compliant with major ATM manufacturers, it is equipped with protective hood to safeguard against bright lights, dust and vandalism. An LED in the casing illuminates to show when the reader is in scanning mode.



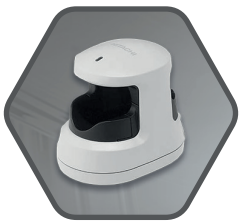
FVID BRANCH PROXY READER

This internet appliance device, based on the FVID Branch Reader, includes special firmware to allow for connections over open networks and is used in conjunction with the Finger Vein Proxy Server. Used by organisations that need to deploy readers outside of their corporate network including banks operating franchise or agency models.



FV BRANCH MONITOR

The FV Branch Monitor is an optional network appliance touch screen monitor, available in a variety of screen sizes and controlled by the Finger Vein Server for the display of relevant customer information during the biometric transaction. Graphical content is displayed to guide the customer through the authentication process. It displays electronic agreements for customer review and acceptance for paperless processing and can be used to display marketing content.



FVID SCANNER

Dedicated for use with PC based applications, this reader is used for logical security applications. Developers can use available software tools to design authentication schemes ranging from simple application level logon access control through to complex transaction level validation. Widely used in enterprise IT and supporting major operating systems it supports one to one and one to many use cases.

FURTHER INFORMATION

Please contact Hitachi Europe Limited for further information about Hitachi's finger vein technology, applications and devices.

CONTACT DETAILS

Information Systems Group,
Hitachi Europe Limited,
Whitebrook Park,
Lower Cookham Road,
Maidenhead,
Berkshire,
SL6 8YA.

digitalsecurity@hitachi-eu.com
http://digitalsecurity.hitachi.eu

HITACHI
Inspire the Next

Hitachi Digital Security