



Enabling
trusted
identities

Result

1.4 million vehicles recalled



Result

114,000 patients warned



Data Security : MasterCard Survey, 2015

Identity Theft: We'd Rather Be Naked



More consumers **(77%)**
are concerned about their financial
information being stolen than:

62%
Email
Hacked



46%
Being
Pickpocketed



59%
Houses
Being Robbed



55%

of Americans would
rather have naked
pictures of themselves
leaked than have their
financial info stolen or
compromised.

Though, What We All **Say** and **Do** Are Two Very Different Things

92% of
consumers feel they
take precautions to
protect their financial
information...



....yet **46%**
rarely (if at all)
change the passwords
on their online
financial accounts.

39% have checked
their personal financial info
on public networks.



Market Insights



Passwords to remember
per user



Loan applications are
not completed



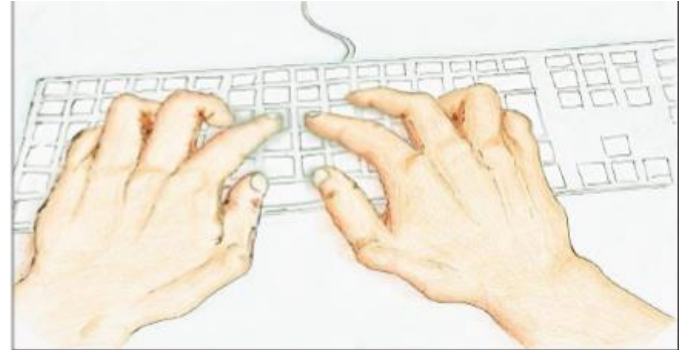
Every 3rd minute an ID is
stolen in Sweden



"I have your MRI results. Half your brain is clogged with passwords and the other half is clogged with user names."

Payment Systems

- SWIFT, private financial messaging platform
- Gather information about Bank's internal procedures for payment transfers, Identity theft(Systems, User name, password, cryptographic keys)
- Social Engineering
- Malware, Trojans
- Keystroke logging, Biometrics



Cybersecurity Framework

- Awareness and strong governance: sensitise the board and management about the evolving threat landscape
- Cyber Resilience: Cyber Crisis Management Plan to address the full life cycle of detection, response, containment and recovery
- Protecting Customers: protecting customer data, customers against financial crimes
- 24x7 security operations centre with adaptive threat defence mechanisms
- Proactive reporting and collaboration: effective cyber security monitoring and detection capabilities
- Cybersecurity Policy: Different from IT/IS Policy

Cybersecurity Controls

- **Inventory Management of Business IT Assets**
 - Hardware/software/network devices, key personnel, services, etc. indicating their business criticality
 - Classify data/information based on information classification/sensitivity criteria of the bank
- **Preventing execution of unauthorised software**
- **Network Management and Security**
 - up-to-date/centralised inventory of authorised devices connected to bank's network (within/outside bank's premises) and authorised devices enabling the bank's network.

Cybersecurity Controls

- **Application Security Life Cycle (ASLC)**
 - security requirements relating to system access control, authentication, transaction authorization, data integrity, system activity logging, audit trail, session management, security event tracking
 - Best practice guidelines: Open Web Application Security Project (OWASP)
- **User Access Control / Management**
 - Implement centralised authentication and authorisation system including enforcement of strong password policy, two-factor/multi-factor authentication depending on risk assessment and following the principle of least privileges and separation of duties.

Cybersecurity Controls

- **Secure mail and messaging systems**
 - Implement secure mail and messaging systems, prevent email spoofing, identical mail domains, protection of attachments, malicious links etc
- **Anti-Phishing**
 - Anti-phishing/anti-rouge app services from external service providers for identifying and taking down phishing websites/rouge applications
- **Risk based transaction monitoring**
 - Risk based transaction monitoring or surveillance process as part of fraud risk management system across all -delivery channels

Software ID - ATM

Designed to stop unapproved
(*unknown and unwanted*) software
from running on protected machines.



21st century
gold rush



Say Hello to Block Chain

- Database file (Tamper evident ledger within a network of entities)
- Keeps history of all the transactions in blocks
- Decentralized, reliable, Cryptographic hash functions & pointers
- Opened to add/read $O(n)$, Closed to delete/modify $O(1)$
- Miners compete to add blocks to it
- Decentralised public Ledger – no trusted third-party
- No central database – blocks of timestamped transactions can be stored on all systems
- Transactions are verified and tracked algorithmically
- Prevents **Double Spending**

Blockchain rush

In 2015 – 2016 45+ financial corporations formed the R3Cev consortium to apply blockchain in financial industry

Barclays, UBS, Bank of America, Deutsche Bank, BBVA, Commonwealth Bank of Australia, Credit Suisse, Goldman Sachs, J.P. Morgan, Royal Bank of Scotland, State Street, BNY Mellon, Citi, Commerzbank, HSBC, Mitsubishi UFJ Financial Group, Morgan Stanley, National Australia Bank, Royal Bank of Canada, SEB, Nordea, Danske Bank, Société Générale, Toronto-Dominion Bank, Mizuho Bank, UniCredit, BNP Paribas, Wells Fargo, ING, Macquarie Group and the Canadian Imperial Bank of Commerce, BMO Financial Group, Intesa Sanpaolo, Natixis, Nomura, Northern Trust, OP Financial Group, Banco Santander, Scotiabank, Sumitomo Mitsui Banking Corporation, U.S. Bancorp, Westpac Banking Corporation, SBI Holdings of Japan, Hana Financial of South Korea, and Bank Itau of Brazil, Toyota Financial Services

In 2015 Linux Foundation started collaborative cross-industry Hyperledger project

Cisco, Digital Asset Holdings, Fujitsu, Hitachi, IBM, Intel, NEC, NTT DATA, Red Hat, VMware, ABN AMRO, ANZ Bank, BNY Mellon, CLS Group, CME Group, The Depository Trust & Clearing Corporation, Deutsche Börse Group, J.P. Morgan, State Street, SWIFT, Wells Fargo, Accenture, Calastone, Credits, Guardtime, IntellectEU, NXT foundation, Symbiont

In 2016 Microsoft, Amazon, IBM started offering cloud sandbox to users for blockchain prototyping

Block Chain : Banking & Finance



Cost Savings , Efficiency & Transparency

Trade Finance

- BCT can address KYC and identity management challenges as a lot of the data to prove identity is already in digital form and BCT could enable instant verification.
- BCT can reduce duplicative recordkeeping, eliminate reconciliation, minimize error rates and facilitate faster payment/asset settlement. Less risk in the financial system and lower capital requirements.
- A trade finance solution with letter of credit, bill of lading and multi-signature solutions based on BCT (Single Version of Digital Truth)

Corporates, shippers, and manufacturers, custom authorities need to be on board

- Carriers issue bill of lading on the BCT as a digital asset
- Banks issue letter of credit / Bank Guarantee as a digital asset on the BCT
- Multi-signature contracts
- Smart-contract-enabled, event-based fund release to ensure speed and transparency

BCT : Banking & Finance

- **Remittances / Payments**

- Interbank transfers
- POS/ATM
- Cross-border transfers
- Alternative to SWIFT

- **Treasury**

- FX Deal , Money Market
- Trading , Clearing , Settlement
- Trade Valuation, Credit Monitoring

- **Lending**

- P2P Lending
- Corporate/Retail Loan
- Mortgage

- **Reporting & Document Management**

- Customer Reporting
- Regulatory Reporting
- Secure Documents & Smart Contracts

Get rid of passwords

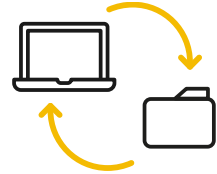


Empower your Business Leveraging further on Existing Channels



Know who you are
talking to?

Digitalize your
work processes



Web

Phone Service

Customer Care

In Person

Authentication: from perimeter to cloud security



PERIMETER SECURITY

- All systems inside firewall
- Remote workforce case
- VPN
- Remote Desktop
- Service Portal
- Enterprise + Employees













CLOUD SECURITY

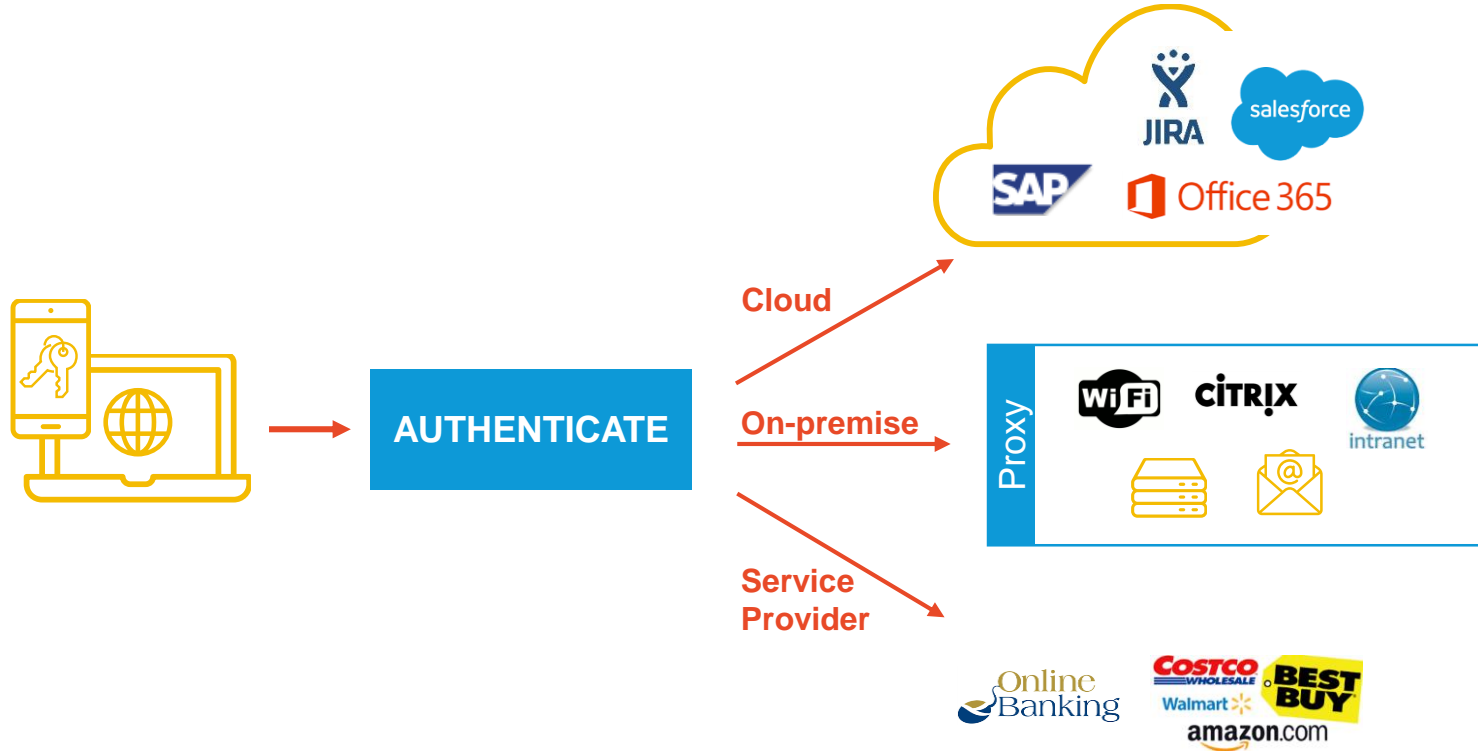
- Perimeter-less federation
- Authenticate once, access many
- Seamless access to multiple independent systems across the network
- Access to Cloud and SaaS-services
- Mobile Two-Factor authentication
- Facilitate use of 3rd party system suppliers in your network
- Employees and consumers



Authentication methods and credentials

	OTP/Email OTP/SMS	Hardware Token	App OTP	Personal Mobile	X509 Certificate
FACTOR 1					
FACTOR 2					
SECURITY	<u>*</u> **	<u>**</u> **	<u>**</u> **	<u>***</u> ***	<u>***</u> **
CONVENIENCE					

Single Sign On and Identity Federation



Identity Orchestration

RE-USE EXISTING IDENTITIES



Seamless use of existing enterprise identity

Pick up identity on first user attach

Active Directory, ADFS, LDAP



UPDATE EXTERNAL SYSTEMS



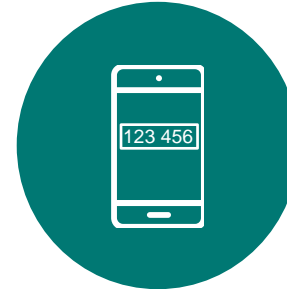
Keep cloud services updated with identity information

Office365, JIRA, Google Apps, Salesforce, ...

SCIM support,
Credential Database



REGISTER AUTHENTICATION METHODS



Prepare authentication methods for first use

Register Personal Mobile app

Set/reset/update passwords