RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: IDY-W02

RISK-BASED APPROACH TO DEPLOYMENT OF OMNICHANNEL BIOMETRICS IN SBERBANK

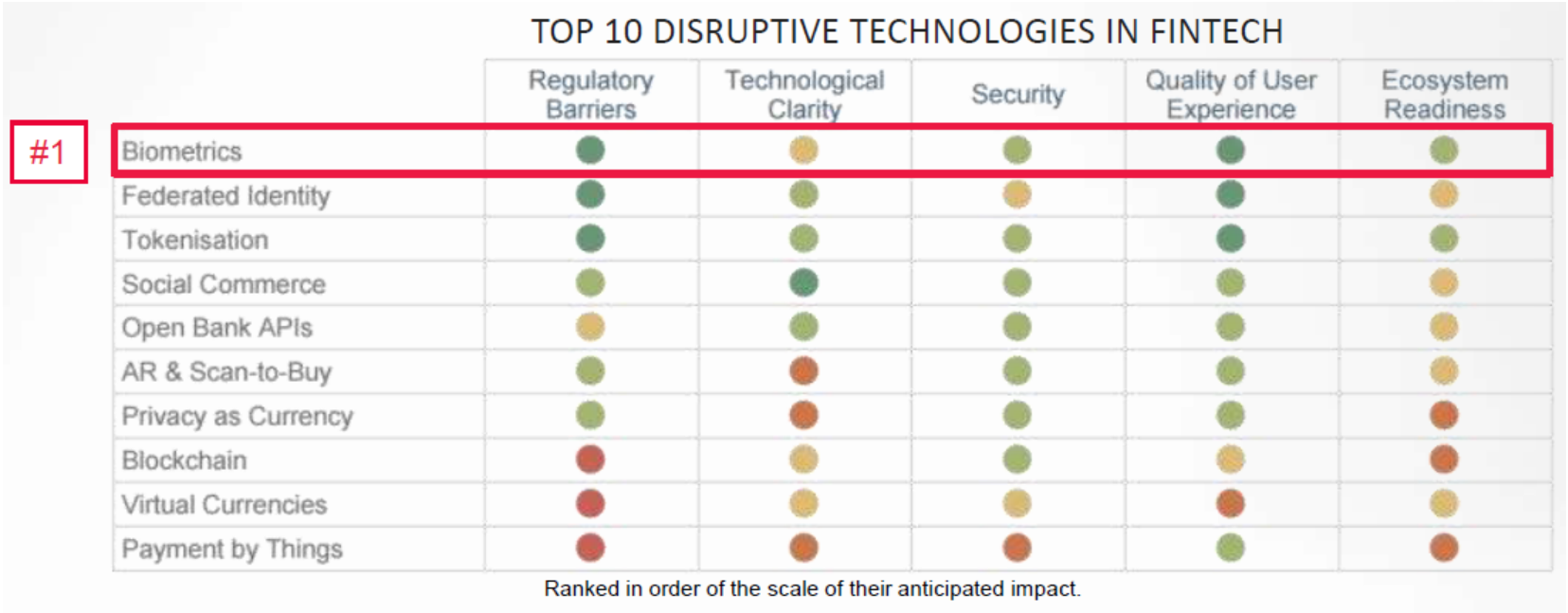
Anton Mitrofanov

Authentication Platform Chief Product Owner
Sberbank

Leyla Goncharenko

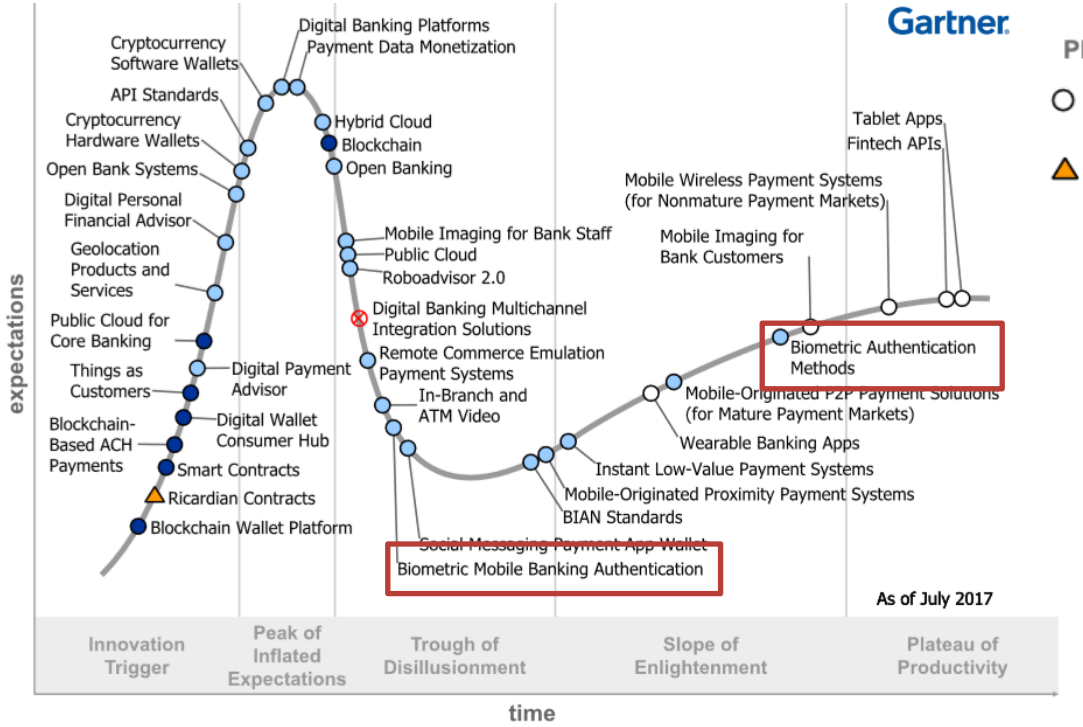
Risk-based authentication Product Owner
Sberbank

Biometrics as a FinTech Trend



Juniper, TOP 10 DISRUPTIVE TECHNOLOGIES IN FINTECH, 2016

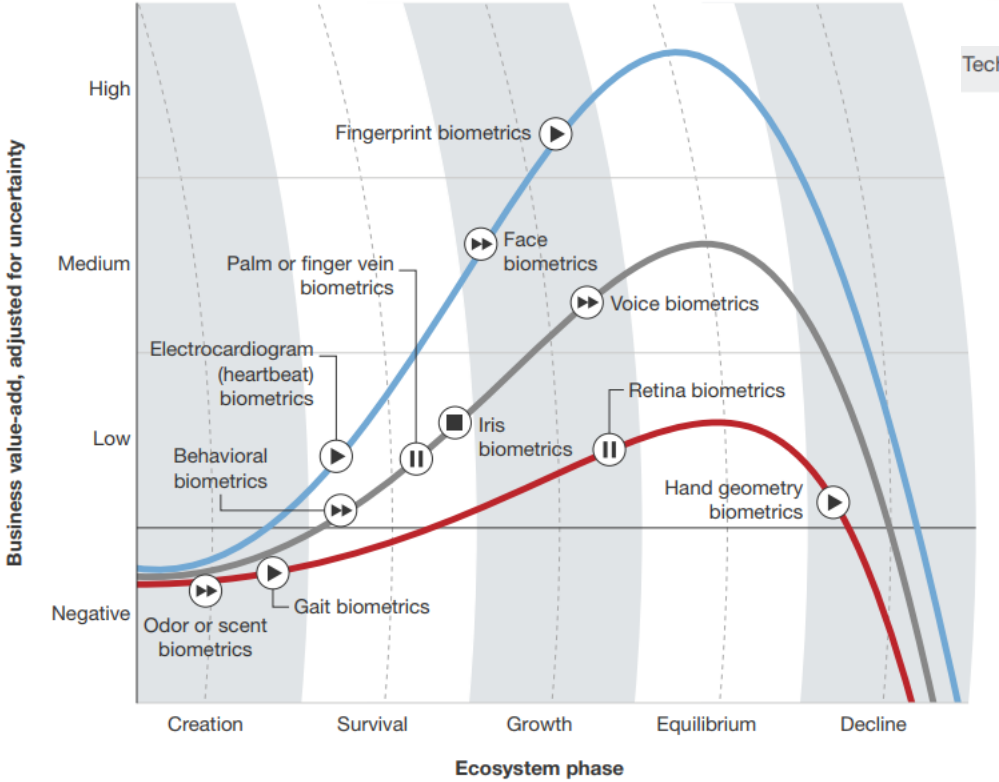
Biometrics as a FinTech Trend



Plateau will be reached:

- ○ less than 2 years
- ● 2 to 5 years
- ● 5 to 10 years
- △ more than 10 years
- ⊗ obsolete before plateau

Biometrics as a FinTech Trend



TechRadar™: Biometric Authentication, Q1 2017

Trajectory:

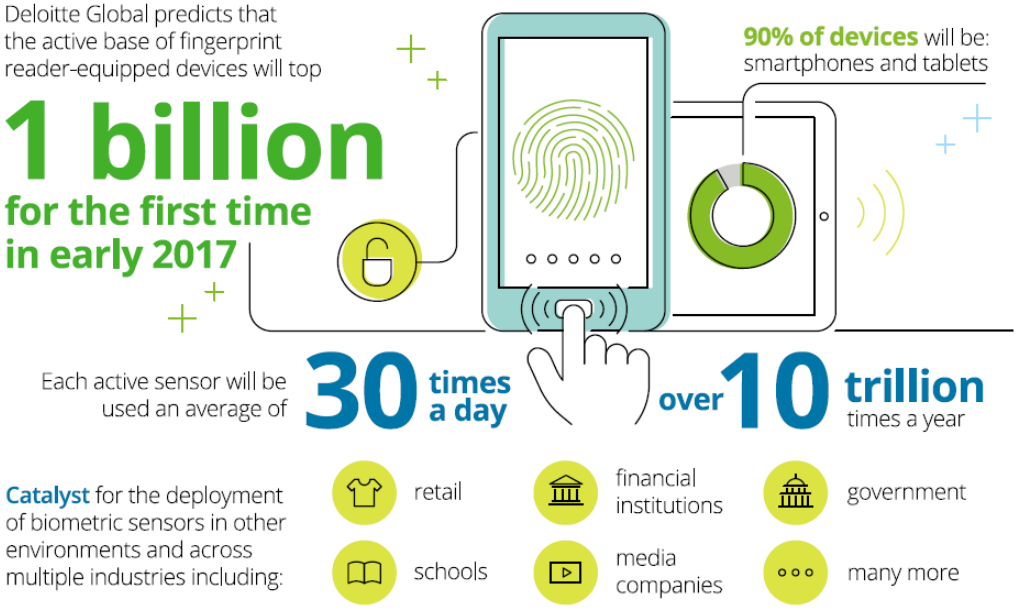
- Significant success
- Moderate success
- Minimal success

Time to reach next phase:

- < 1 year
- 1 to 3 years
- 3 to 5 years
- 5 to 10 years
- > 10 years

Biometrics as a FinTech Trend

Prints charming: biometric security reaches the billions



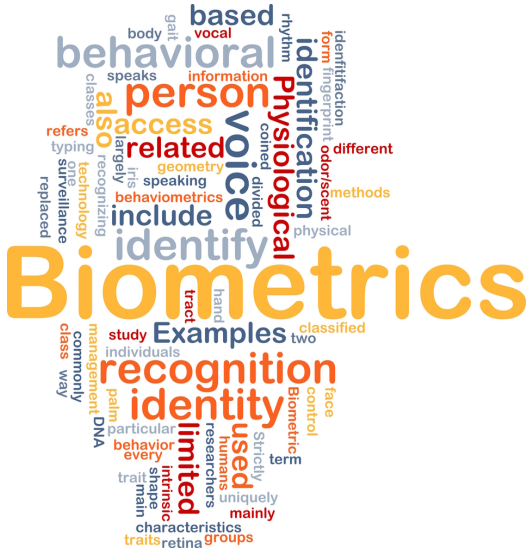
Deloitte.

#DeloittePredicts

Biometrics as a FinTech Trend

- Banks turn into digital platforms
- Digital UX requires seamless and fast security– biometrics?
- Biometrics is already trendy among mobile devices (FaceID, TouchID)
- Banks experimenting with different types of biometrics depending on the environment (Branch, Call Center, Mobile Apps, ATM)
- Biometrics becomes a part of government regulations and complience

Biometrics is a “silver bullet” ..?



- No need to take the IDs - Biometrics is always with you
- Biometrics aligns the Customer experience among the service channels:
  - ATM
  - Branch
  - Mobile Apps
  - Call Center
- Getting the costs down for the branches and call center

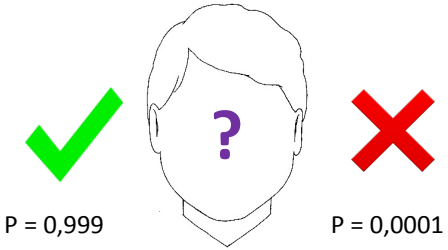
.. Or a challenge?

What the Banks face when implementing biometrics are:

- Privacy concerns
- Liveness issues
- Recognition accuracy
- Enrollment is not equally secure
- Complicated rules and trust matrix are implemented to reduce the risks

Biometrics limitations

Recognition accuracy



Probability of false accept for biometrics is always above zero

Accuracy in large volumes

Is it alive?

Biometrics based mostly on image processing. How could we assure that it is live person?

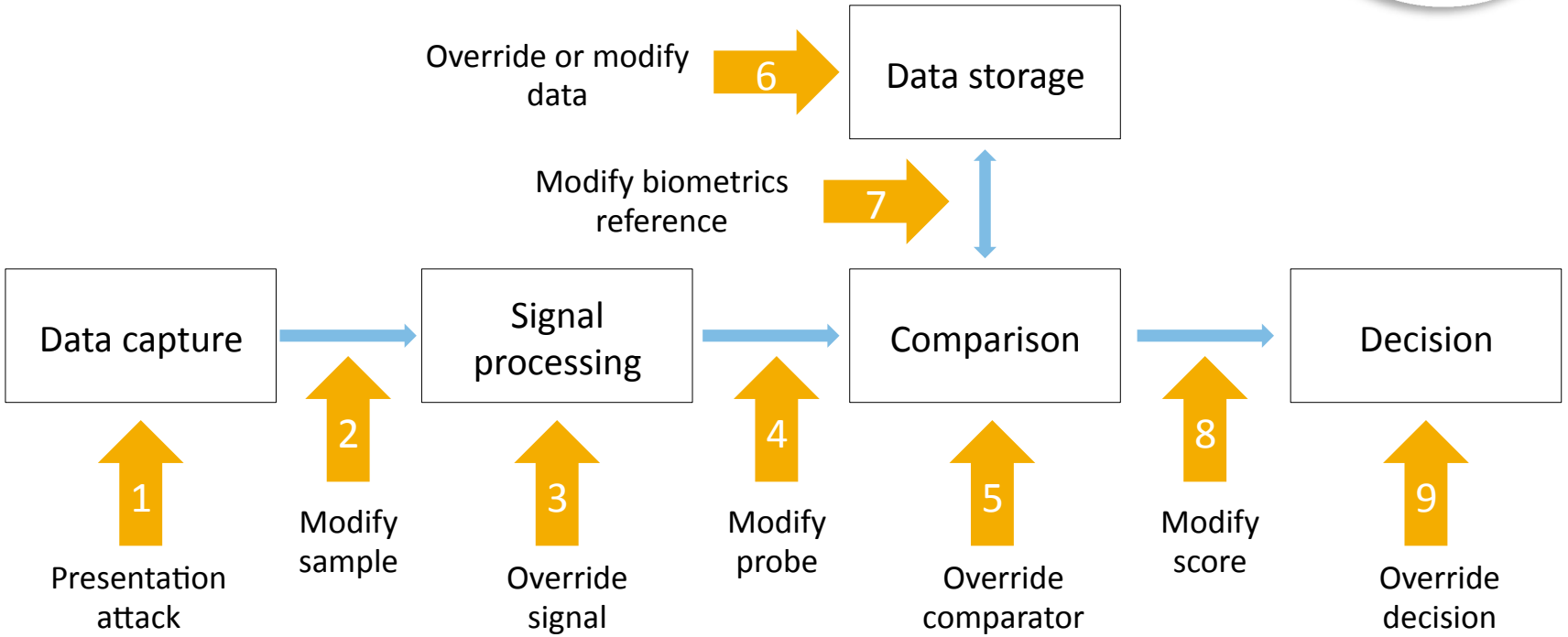
How to re-issue your biometrics?

If your biometrics was stolen - how could we trust you?

SBERBANK

RSAConference2018

Biometrics technologies security Framework



From ISO/IEC 30107-1, inspired by figure by Nalini Ratha from 2001 and Standing Document 11 of ISO/IEC JTC1 SC37.

Biometrics technologies security
Attacks examples

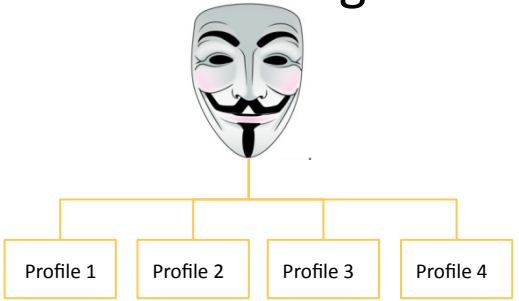
Biometrics scanners
Spoofing

Presentation attack

Biometrics search engine
Morphing

Override comparator

Enrollment process
Profile stealing



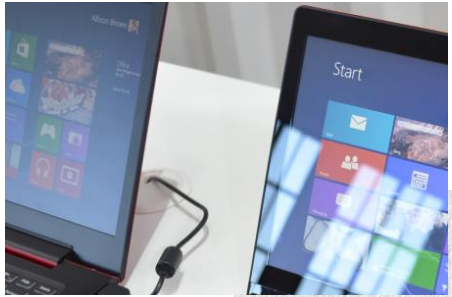
Modify biometrics reference

Biometrics liveness detection

Interactive liveness

- Random user actions
- «3D» models based on movements

Environmental liveness

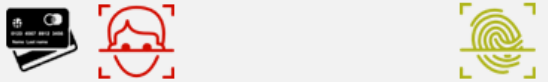
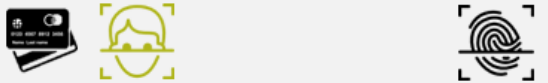


- Recognition of displays signatures
- Recognition of paper and phone/ tablet forms

Scanner-based liveness

- 3D models based on depth
- surface, temperature and pulse analysis
- IR images

Authentication factors across the channels

Channels	ID / Authenticators	Considerations
Branches		Fingerprint may be reused even without scanner
Call Center - operator		Text-independent may be reused between CC and IVR, it is also good for black or white list monitoring
Call Center– IVR		Text-dependent requires some action from a user, but it is more feasible in IVR, remote banking, etc.
Remote Banking / OpenAPI		Behavioral biometrics may be used as a second factor or as a source for fraud monitoring
ATM / Self-Service Kiosks		Though fingerprint and palm veins are most commonly used, we see a lot of potential in face
Acquiring		Biometrics in acquiring is limited to availability of devices. Fingerprint is most commonly used, but new models with cameras become availiable.

Lessons Learned

- Voice and face biometrics are easier to integrate and common for Customers.
- Behavioral biometrics is an additional invisible layer of protection.
- Fingerprints and palm veins – good for physical access and trade acquiring.
- Presentation attack detection is still a challenge: we see potential in multimodal liveness detection (e.g. face+voice or face+behavior).
- Server-side processing provides omnichannel approach, but still you need to estimate the risks.
- On-device processing is still on our radar as the privacy concerns and regulations may change the world quickly

RISK-BASED AUTHENTICATION AS UNIVERSAL SOLUTION

Risk-based authentication
Basic workflow

1. Score action's risk level
   - Risk score
   - User behavior profile for anomaly detection
2. Select available auth factors
   - Define available auth factors
   - Check IT-environment for scanners availability
   - Select appropriate combinations
3. Define necessary and sufficient challenge
   - Define challenge based on risk score

   Factor i weight F_i

   Risk score R

   Challenge: Sum (F_i) – R = 0
4. Authenticate by selected factors
   - Challenge user by selected factors
   - Confirm users identity

Measuring risks

Authentication data model

- Behavior profile
- Environment data
- End-point device fingerprint
- Action data

Authentication measurement models

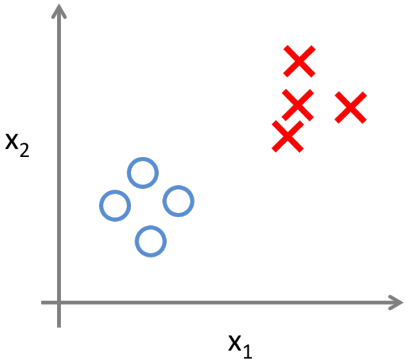
- Anomaly behavior
- Change in environment
- End-point device fingerprinting
- Action risk scoring

Rule-engine decision maker

- Set thresholds for interpreting measurement results
- Rules for combining results of measurements
- Rules for including external data and models results
- Decision making conveyer

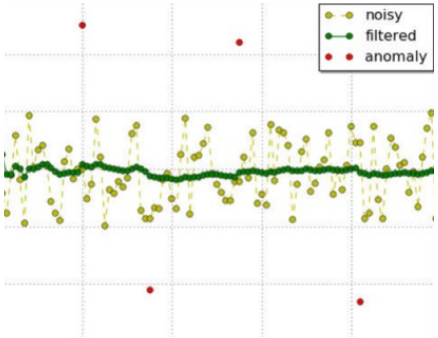
How to measure auth attempt?

Supervised learning



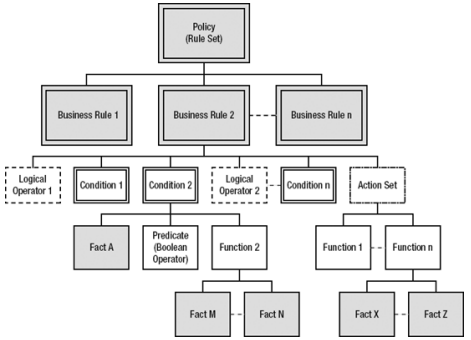
Based on appeals from customers or IDS/Fraud incidents detection

Unsupervised learning



User behavior profile for anomaly detection

Rule engine

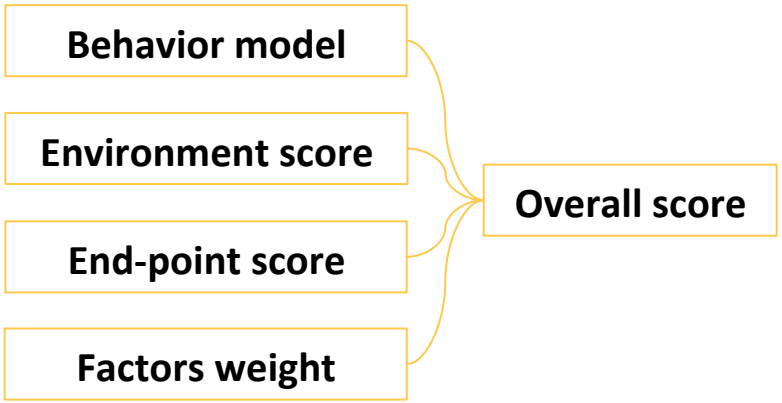


Set of rules, describing:

- know attacks/frauds
- interpretation of outputs from models

Authentication measurement models

- User behavior scoring looks at previously aggregated statistics of typical user actions
- Environment scoring based on geolocation, network provider, IP
- End-point device scoring takes into account device attributes (model, S/N, hardware etc)
- Rule-engine as mandatory component of decision making for risk-based approach – our approach to use rules for interpreting scores from models

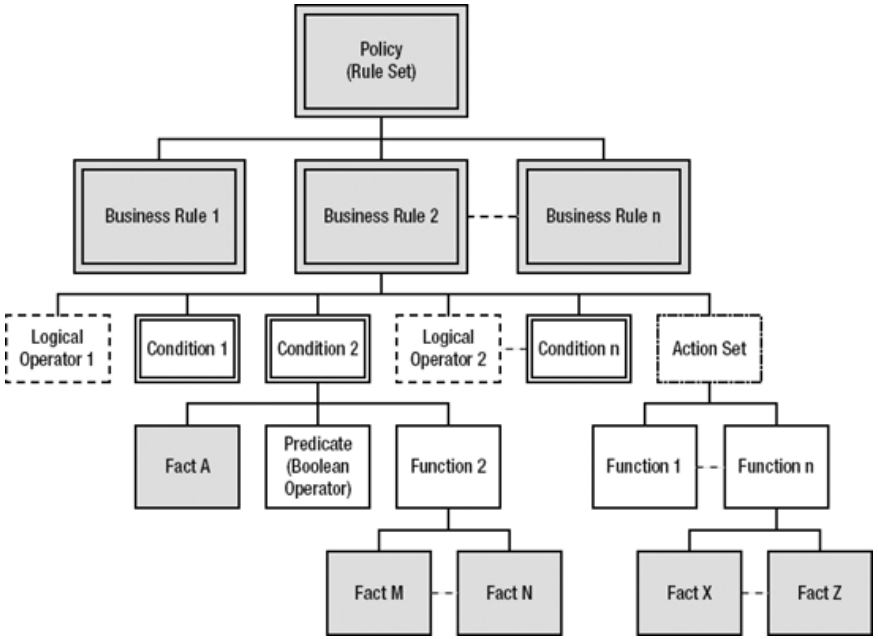


Rule-engine for risk-based models

Rule-engine is mandatory component of decision making for risk-based approach

Rule-engine used for:

- Interpreting models scoring
- Defining known attack/fraud cases
- Selecting available and allowable authentication factor
- Composing final decision



How to measure auth factor's trust?

- Frequency of usage by user – how usual this factor is for this user?
- «Resistance» to compromising (based on experience) – set by security experts based on best world practices and experience
- Channel type – how secure is channel of registration?
- Attack statistics – how much security incidents with this type of factors?

How to measure biometrics template's trust?

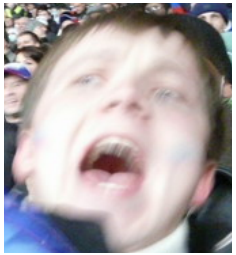
- Biometrics template enrollment channel
- Step-up bio template confirmation
- Step-up template confirmation process

VS

?

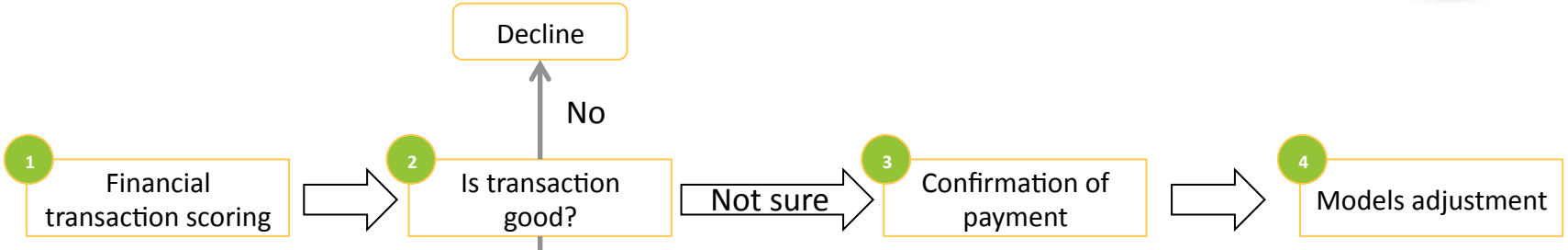
- Biometrics enrollment sample quality
- Liveness detector score
- Enrollment environment risk score

VS



?

Risk-based transaction verification



- Transaction risk score
- Authentication risk score
- User environment, etc.

- Transaction risk score
- Authentication risk score
- User environment, etc.

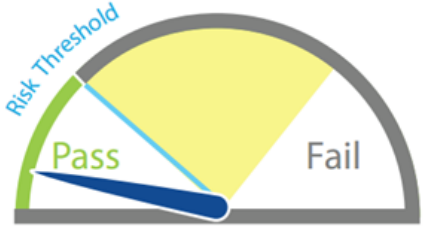
- What factors available in this channel?
- What factors are available for user?
- Supposed fraud case restricts sufficient auth factors
- What factors set are sufficient to ensure trust?

- Adjusting transaction and authentication measurement models according to confirmation result

RBA: Typical transaction

Legitimate user makes a typical transaction in a banking mobile app

RBA checks the pre-requisites					
Login+pass	Device "fingerprint"	Geolocation, IP-address, etc.	Behaviour pattern	Transaction metadata	Metadata from the other systems
Current operation pattern:					
Entered correctly from the first try	Known device with a good background info	Typical geolocation and IP-address	Typical behavioral pattern	Typical transaction	No red-flags from the other systems, e.g. SIM-card never switched, mobile number never changed, no SIEM alerts, etc.



User Risk: low **Transaction risk:** low

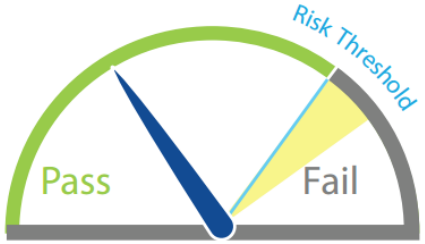
Action: allow transaction

Result: transaction allowed with no additional actions from a user

RBA: Step-Up and De-escalation

Legitimate user makes purchase abroad

RBA checks the pre-requisites					
Login+pass	Device "fingerprint"	Geolocation, IP-address, etc.	Behaviour pattern	Transcation metadata	Metadata from the other systems
Current operation pattern:					
					
Entered correctly from the first try	Known device with a good background info	Non-Typical geolocation and IP-address	Typical behavioral pattern	New transaction type, but no fraud-signs detected	No red-flags from the other systems, e.g. SIM-card never switched, mobile number never changed, no SIEM alerts, etc.

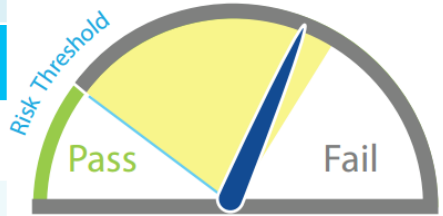


User Risk: low or medium **Transaction risk:** medium
Action: allow transaction or request step-up using additional factor
Result: transaction allowed after two-factor authentication

RBA: Fraud Prevention

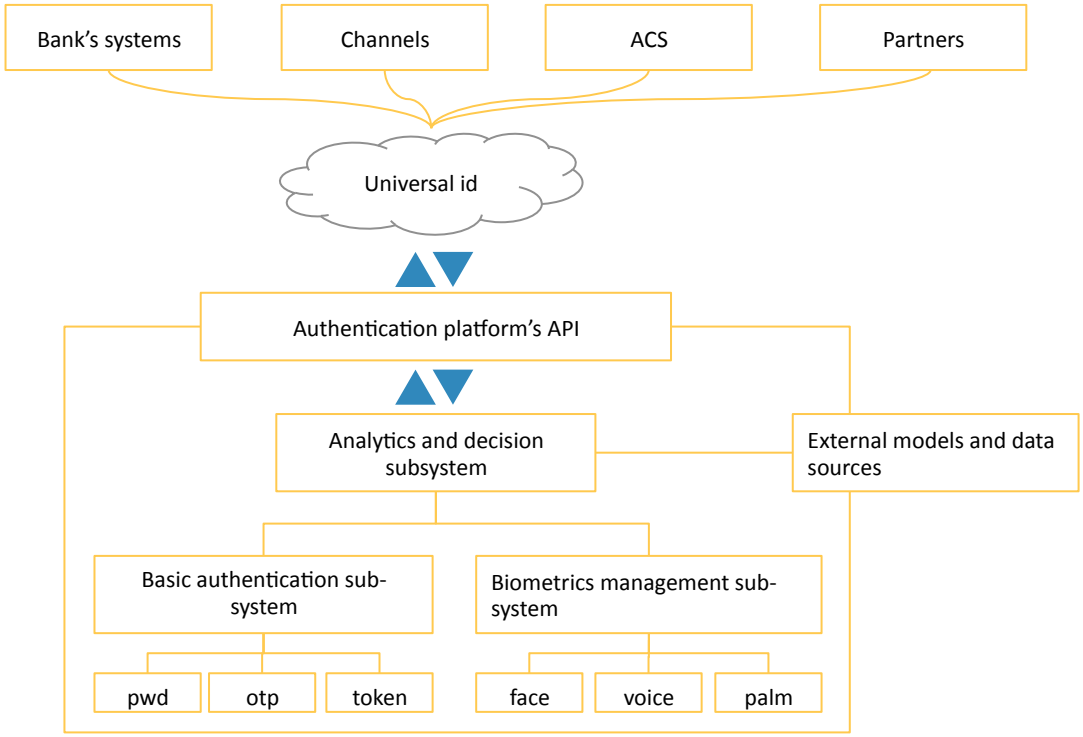
Fraudster attempts to make non-legal transaction

RBA checks the pre-requisites					
Login+pass	Device "fingerprint"	Geolocation, IP-address, etc.	Behaviour pattern	Transaction metadata	Metadata from the other systems
Current operation pattern:					
					
Entered correctly from the first try	New device, no background or red-flags.	Non-typical geolocation and IP-address	Non-typical behavior	Risky transaction and/or fraud signs	Red alerts from the other systems: e.g. new mobile number was added recently



User Risk: high **Transaction risk:** high
Action: request step-up using additional factor
Result: transaction denied because of authentication failure

Unified authentication platform concept



Key principles

- Action's risk measurement
- Dynamic challenge selection
- Multifactor authentication
- Multimodal biometrics

Biometrics role

- Additional trust factor for ID
- One of the many authentication factors
- Comfortable tool for end-users

Next steps for application

- Identify and categorize all the authentication options used
- Identify all channels, where authentication is needed
- Create matrix of applicability for channels and auth factor
- Set weight's for auth factors in each channel
- Biometric tuning is a must
- Integrate biometrics with IAM and fraud-monitoring solutions

THANKS!
QUESTIONS?

Anton Mitrofanov

admitrofanov@sberbank.ru

Leyla Goncharenko

lkhgoncharenko@sberbank.ru