SPEECHPRO

Biometric Authentication

Bringing End users and Enterprise on the same page

ABOUT SPEECHPRO

▶ **SpeechPro** is a World Leader in Speech Technology with customers in 75 countries

▶ **SpeechPro** is part of the global company with over 20 years of experience
  - ▶ **Strong R&D** with over 30 PhD's in the team (150 employees in R&D alone)
  - ▶ Full suit of proprietary algorithms (see **NIST** results for accuracy)
  - ▶ **Star Performer 2014** by Speech Technology Magazine
  - ▶ Compliant with Avaya, Cisco, Genesys, Aspect
  - ▶ ISO 9001 Certification

Congratulations!

Voice Biometric Technology works!

Hurray!!!

SO WHY AREN'T MORE PEOPLE USING IT?

Mighty enemy – Password!

- ▶ Inertia
- ▶ Perceived complexity of implementation
- ▶ Perceived lack of accuracy vs KBA
- ▶ Privacy concerns

2 key demographics

End Users

Enterprise Integrators

Need to enhance user experience

KNOW YOUR ENEMY

- ▶ What do we compete against?
- ▶ How well do passwords work?
- ▶ What makes for a good authentication experience?

Security
Usability
Va va voom – fun!

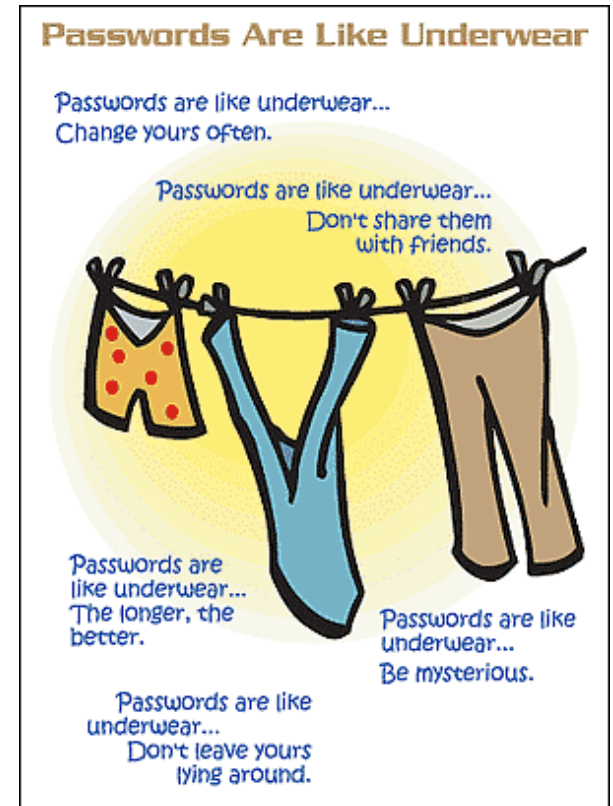**Knowledge-based authentication:** (KBA) — passwords and security questions

- ▶ 10-25 % of legitimate users, fail to answer the questions correctly or forget passwords
- ▶ Fraudsters correctly respond by using culled or stolen information, social engineering.
- ▶ Password depositories are under threat of hacker attacks
- ▶ Authentication of an information not a user

USABILITY - PASSWORD FATIGUE

- 38% - 1 password for all accounts

- 58% of adults have 5 or more online passwords

- 30% - 10 or more passwords

- 8% has 21 or more individual passwords

- **Passwords are getting more and more complicated**

Is this convenient for a user?

Passwords Are Like Underwear

Passwords are like underwear...
Change yours often.

Passwords are like underwear...
Don't share them with friends.

Passwords are like underwear...
The longer, the better.

Passwords are like underwear...
Be mysterious.

Passwords are like underwear...
Don't leave yours lying around.

USABILITY - PASSWORD NIGHTMARES

- Adults age 55 or older on average have 8.2 passwords
- Millennials (18-34 year olds) average 6.7 passwords
- Adults age 35-44 average 8.7 unique passwords
- Adults 45-54 have 8.4 passwords on average
- Men age 45-54 have the highest average number of unique passwords at 9.8
- **37% users ask for assistance on their user name or password for at least one website per month***

Is this a good customer experience?

Harris Interactive

FUN, 2000 YEARS IN THE RUNNING

▶ Password - word or string of characters used for

  user authentication.

▶ Invented by the Roman Empire as a watchword

▶ Identifies a word, not a user

▶ "Knowledge Based Authentication" (KBA) – information

  vs individual

Should we update our security protocol?

NEW, MOBILE REALITY

▶ **Smartphones everywhere**

- ▶ Over a billion smartphones used now, 3 billion by 2017
- ▶ Transactions going mobile
- ▶ 20% of all online transactions are mobile (11% - 2012)

▶ **BYOD movement**

- ▶ *Bad news* - Cross platform environment
- ▶ *Good news* - New technological capabilities available on devices

▶ **Biometric devices in the hands of a consumer**

- ▶ Microphone
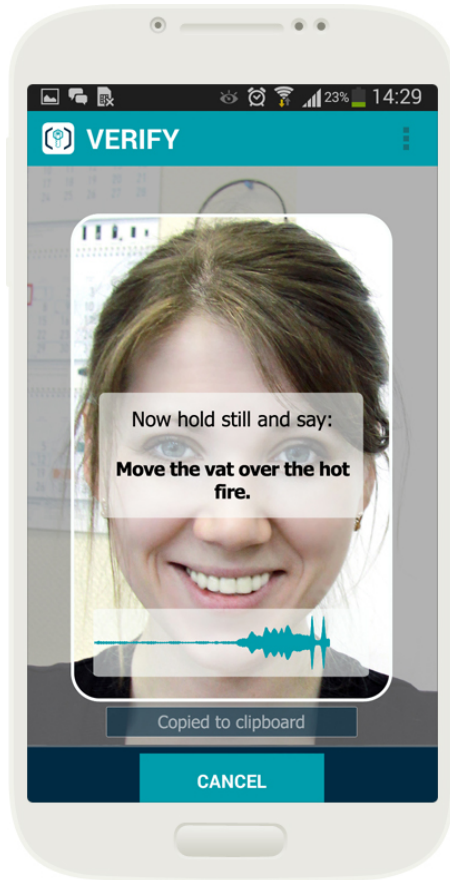- ▶ Camera
- ▶ Screen

<u>Multimodal</u> biometrics without additional hardware

SECURITY. VOICE + FACE = UNIQUE ACCURACY
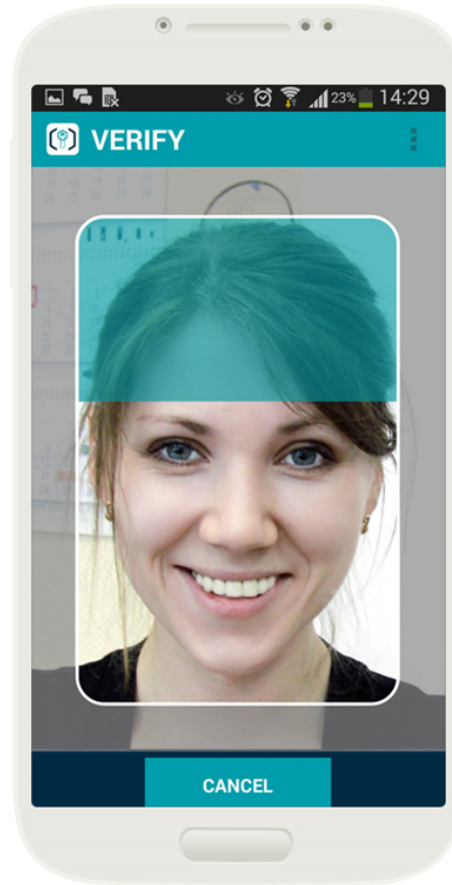
MULTI-MODAL APPROACH DRASTICALLY REDUCES EER
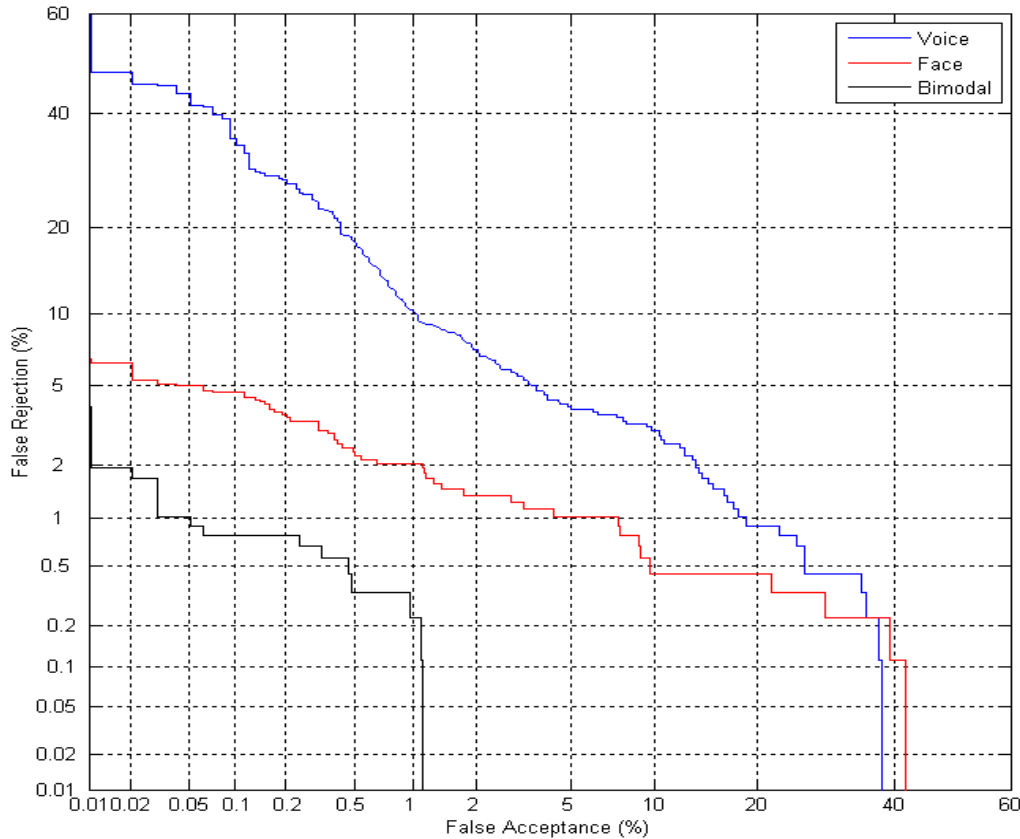
▶ **EER under 0.5% for multi-modal verification in real life environment**
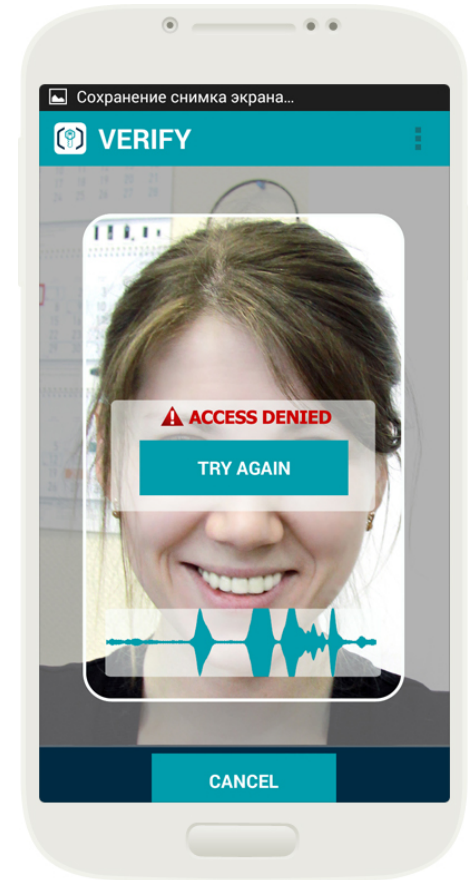
▶ **FA – 0.01% with FR under 2%**

USABILITY. 3-5 SECONDS BIOMETRIC ID

Collect   **Process**   **Access/Deny**

HOW DOES IT WORK?

How Does ONEPASS Work?

30 SECOND ENROLLMENT Take one picture and record 3 short utterances (passwords).

3 SECOND VERIFICATION When a user tries to access a secure service or content, OnePass asks the user to pronounce a password and takes a smartphone picture of their face at the same time, providing multi-biometric data collection with just one click.

SECURE PROCESSING The voice and image templates are formatted algorithmically and sent to the cloud for processing.

INSTANT ACCESS If the matching results are positive, the user gains access; if not, access is denied

CLOUD

Access granted

Access denied

ANTI-SPOOFING
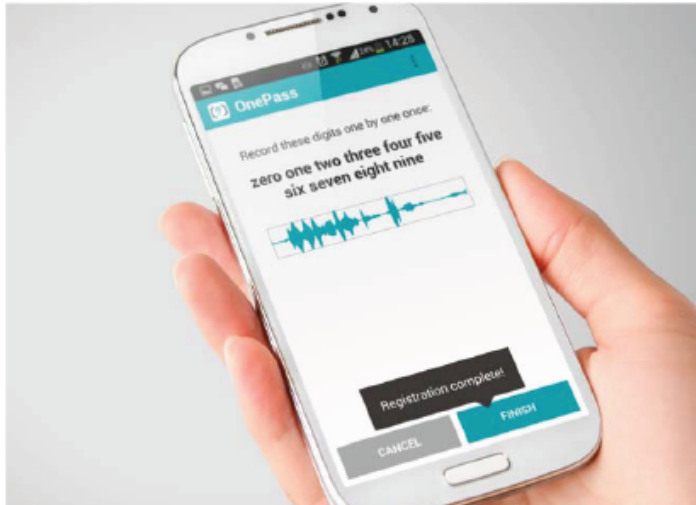
## Triple Biometric Accuracy and Liveness Detection

- Ensures a photograph or voice recording is not used for authentication
- Tracks mouth movements for face authentication
- Prompts for random passphrase for voice authentication
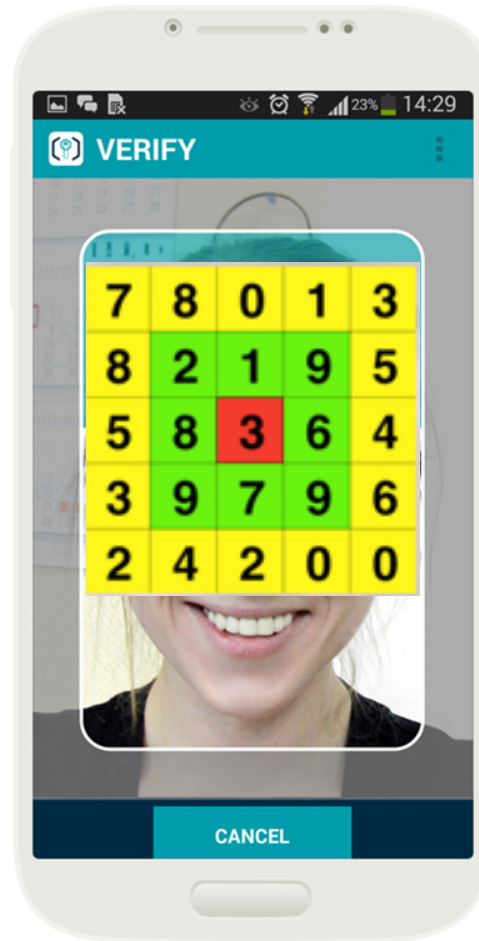
DYNAMIC PASSWORD

- ▶ Customer feedback – anxiety about displaying combination on the screen.
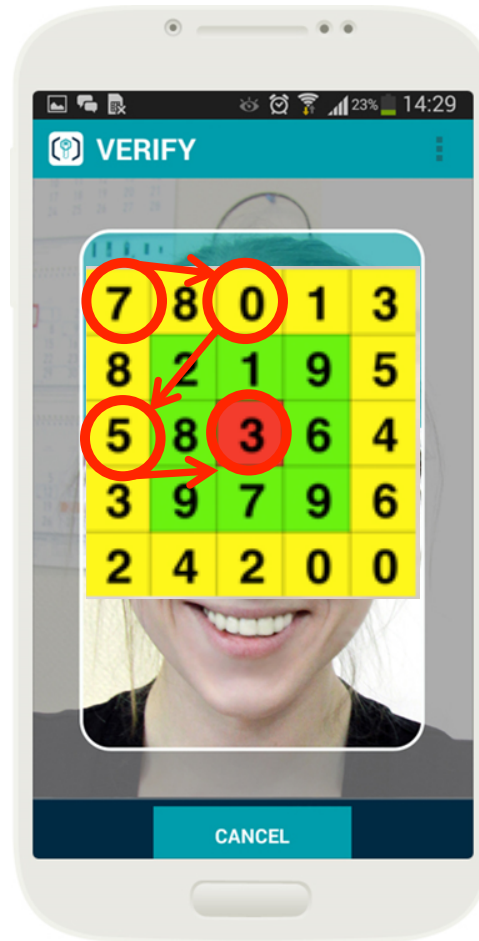- ▶ Screen is a communication tool
- ▶ Let's have fun!

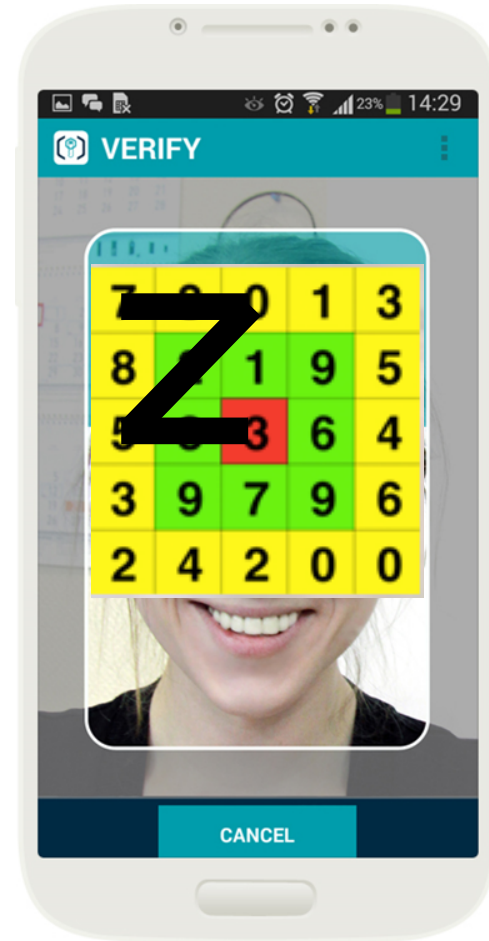# TRADITIONAL PROMPTED COMBINATION
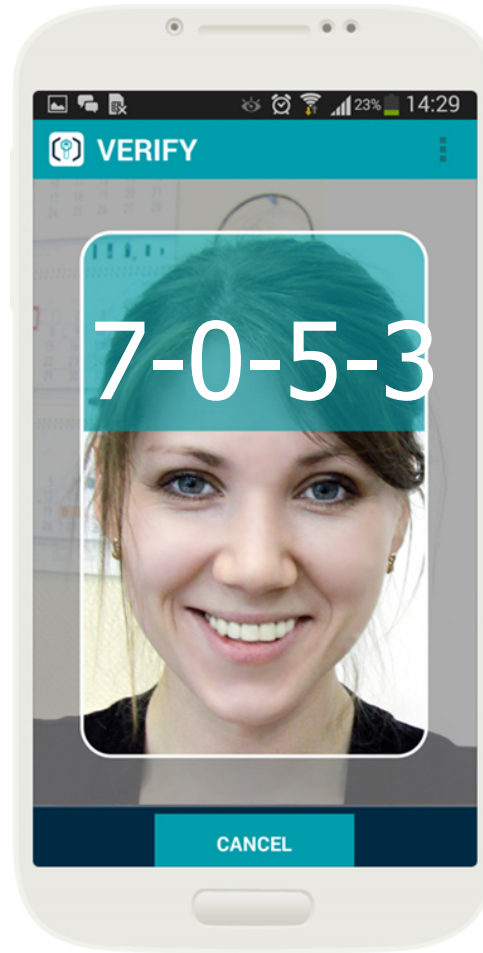
CAN YOU TELL MY COMBINATION NOW?

YOU ARE THE ONLY ONE IN THE KNOW!

REMEMBER THE PATTERN, NOT WORDS

▶ Visual Clues as a security factor
▶ KBA meets biometrics on mobile platform
▶ Multifactor security solution
▶ User friendly
▶ Individual customization

LET'S TRY DIFFERENT PICTURE

YOU SEE WHAT OTHERS DON'T

TRIPLE FACTOR BIOMETRICS

- ▶ Voice Biometrics
- ▶ Knowledge Based Authentication
- ▶ Facial Recognition
- ▶ Anti-spoofing

Secure User-friendly Fun

- ▶ *Available in 2015*
- ▶ *Patent pending*

BUT…

USER EXPERIENCE LEADS TO COMPLEXITY

- ▶ Biometric options drastically increase complexity of authentication deployments
  - ▶ Text Dependednt vs Text Independent
  - ▶ Static vs Dynamic
  - ▶ Passive vs Active
  - ▶ Voice vs Biomodal
  - ▶ Client vs Server
  - ▶ Cloud vs premise
  - ▶ SDK, API, DB, compliance, high availability…
- ▶ Vendors are guilty of perpetual complexity with myriad of products that address specific scenario or need, but require additional integration efforts from enterprise users.
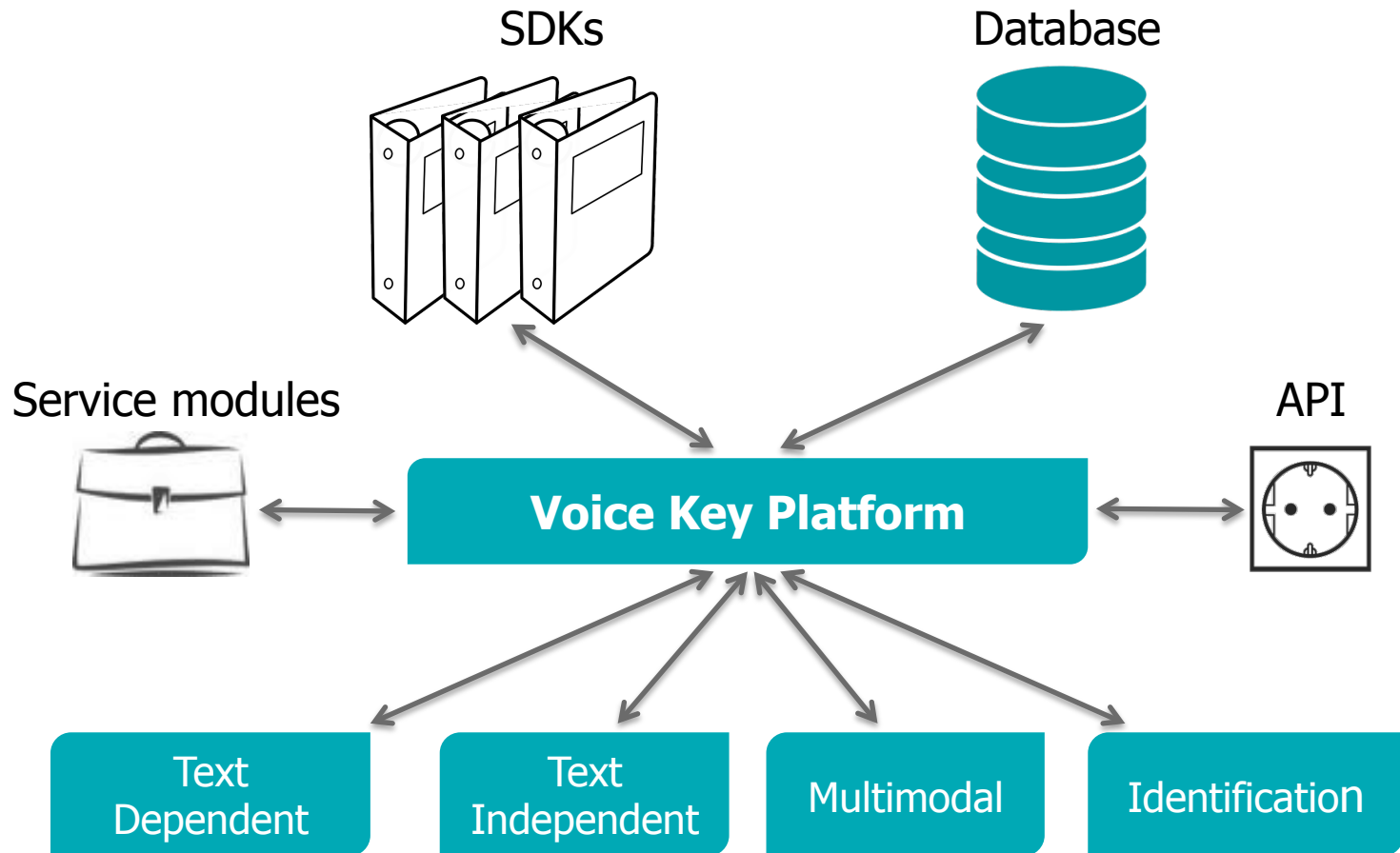
CURRENT SITUATION

- ▶ Various proprietary solutions for various applications and scenarios
- ▶ Myriad products
- ▶ Rigid architecture
- ▶ No unified deployment and maintenance procedures
- ▶ No unified integration API
- ▶ Variety of service tools not included (load balancer, security manager etc.)

What can make life easier?

- ▶ All-in-one approach
- ▶ One technological platform for the all biometric products.
- ▶ Unified architecture
- ▶ Scalability
- ▶ Ability to easily maintain and to update
- ▶ Flexibility to add new features/modules
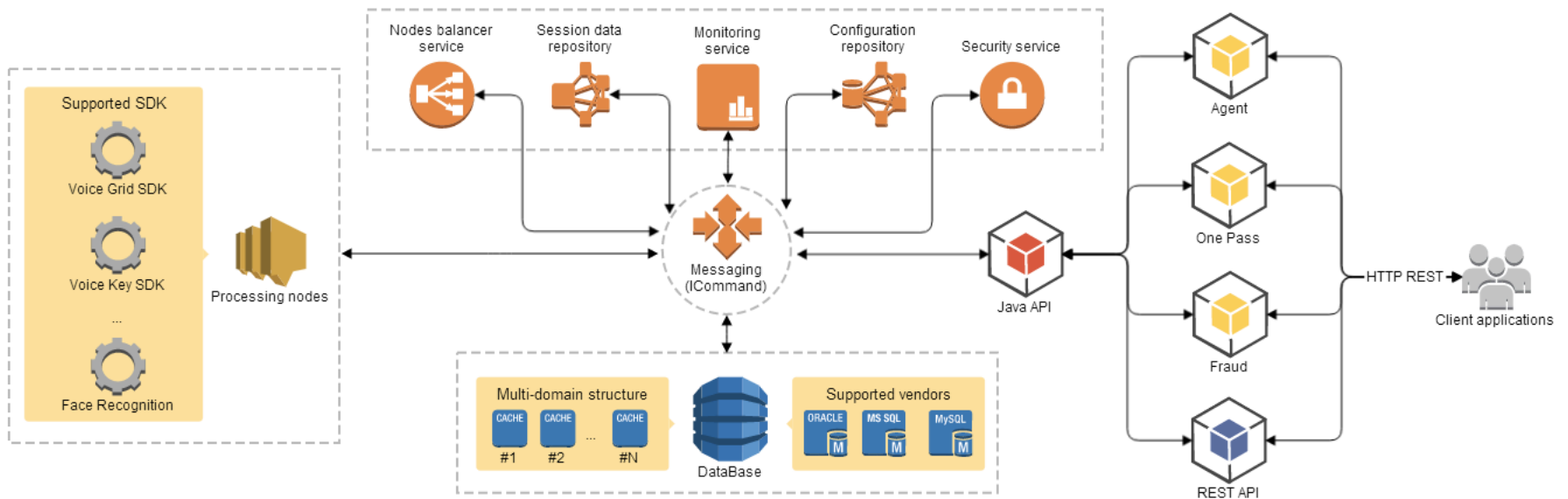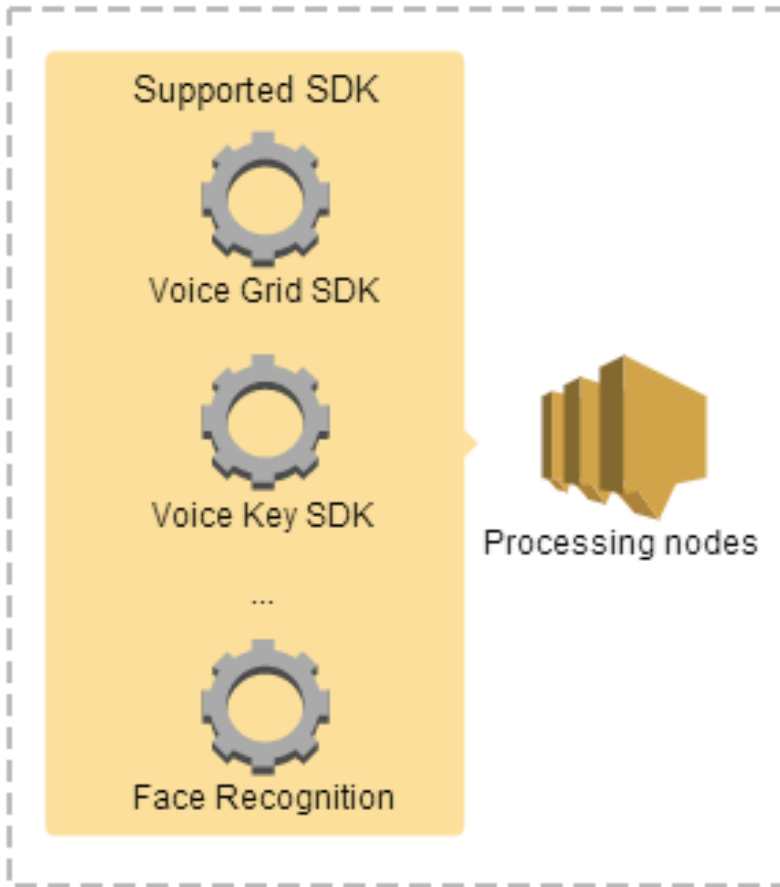- ▶ Unified integration API

INTRODUCING - VOICEKEY PLATFORM

SDKs

Database

Service modules

Voice Key Platform

API

Text Dependent

Text Independent

Multimodal

Identification

VOICEKEY PLATFORM ARCHITECTURE
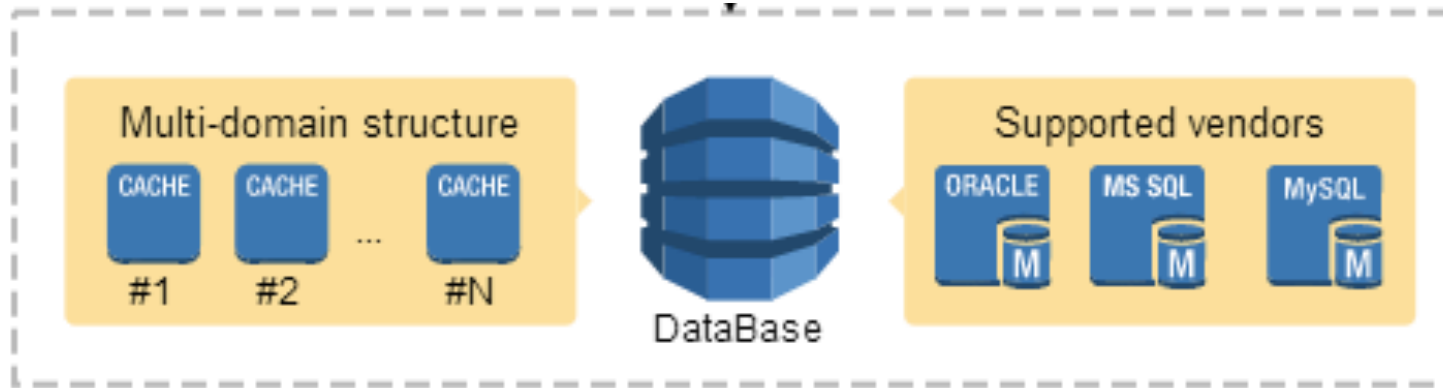
VOICEKEY PLATFORM ARCHITECTURE

PROCESSING NODES

- ▶ Each node contains an instance of specific SDK
- ▶ Set of SDKs may vary and depends on the customer's needs
- ▶ Processing speed can be increased by adding new nodes and maintaining of the workload balance using Nodes Balancer Service

DATABASE

- ▶ Contains metadata and voice models with the assigned ID
- ▶ No personal data is contained in the database
- ▶ Oracle, MS SQL, My SQL and virtually any RDMS are supported
- ▶ Logical separation between domains (customers, departments etc.)

SERVICES
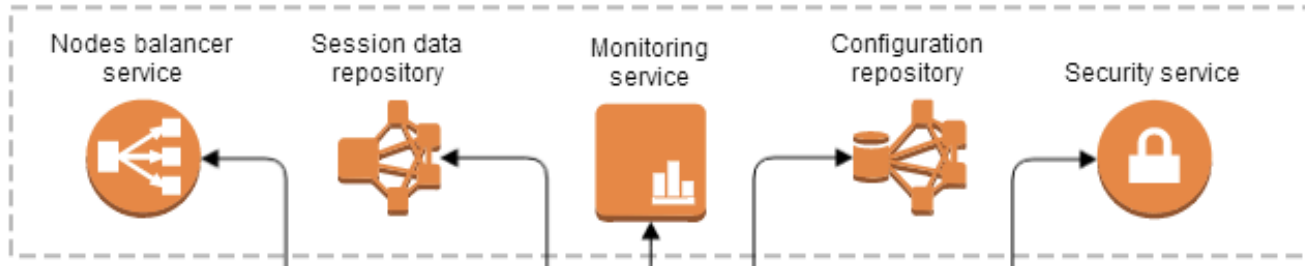
Nodes balancer service
- ▶ Manages the nodes workload rules
- ▶ Distributes the requests among the appropriate nodes

Monitoring
- ▶ Generates reports regarding the condition of different components within the Platform
- ▶ Provides centralized management features of the all components within the Platform
- ▶ Provides an interface to integrate with monitoring applications such as Zabbix

Configuration repository
- ▶ Keeps settings of each component within the Platform
- ▶ Provides UI for the centralized settings management

Security service
- ▶ Defines areas of visibility of the biometric data for the users
- ▶ Defines available scenarios for the users
- ▶ Manages users' sessions

VOICEKEY PLATFORM ESTIMATED TIMELINE

VoiceKey SDK enhancements

March 2014
Start of SDK Enhancement projects

October 2014
Algorithms enhancement:
- Speech recognition for the password phrase
- Enhanced liveness detection
- Video detection

November 2014
Android and iOS Demos.
End of SDK enhancement project

VoiceKey Platform development

September 2014
Start of VoiceKey development project

December 2014
VoiceKey Platform 1.0:
- Messaging
- Processing Nodes
- Database
- Node Balancer Service
- Session Data Repository
- Security Service
- Java API
- REST API
- Documentation

Q 1 2015
OnePass migration to VoiceKey Platform
- Demos
- Documentation
- Presale Toolkit

Q2 2015
VoiceKey Platform 2.0
- Monitoring Service
- Configuration repository
- Deployment package
- Bug fixes

Q 3 2015
VoiceKey Platform 3.0
- Improvements
- Bug fixes

IN CONCLUSION...

▶ End users and Enterprise are very much alike.

▶ Both want a secure and user friendly experience

Let's kill the passwords!
▶ We can do it!

▶ 2015 – year of voice biometrics!

THANK YOU!