RAZ-LEE

iSecurity Multi Factor Authentication

iSecurity
Multi Factor Authentication

Our MFA works based on Persons

"One simple action you can take to prevent **99.9%** of attacks on your accounts"

Melanie Maynes, Director of Product Marketing Manager

Microsoft Security

RAZ-LEE

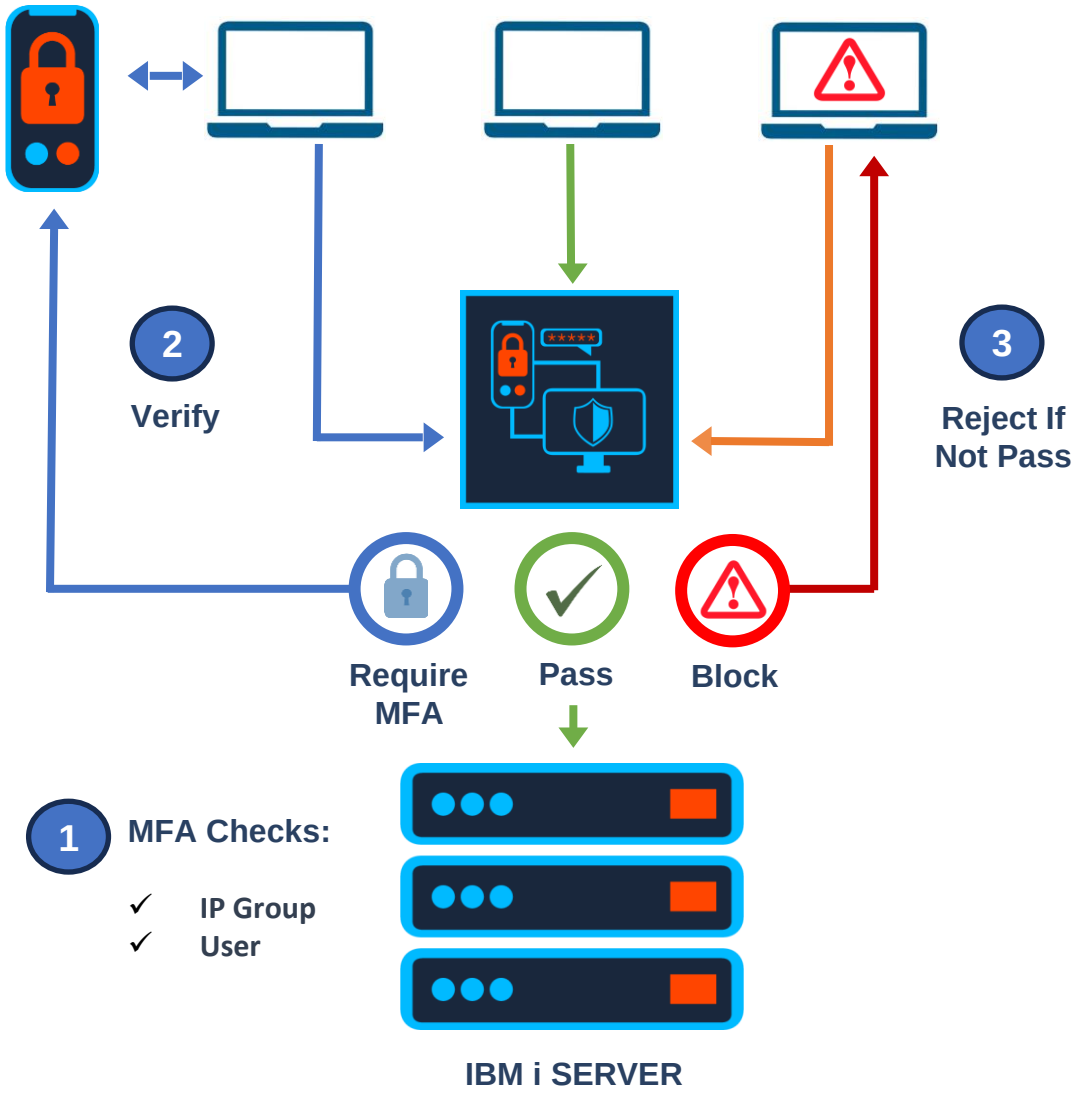
Do I need Multi-Factor Authentication?

iSecurity Multi-Factor Authentication helps your organization meet compliance standards like **PCI-DSS, NIS2, DORA**, etc. and improve the existing security environment on IBM i.

It requires the user, before gaining access to sensitive systems and data, to verify his or her identity with an additional credential.

Such additional credential is usually based on something he has (cell phone, email…) or something he is (fingerprint, face recognition…).

Lately **MFA** has also become a necessity to qualify for cyber insurance.

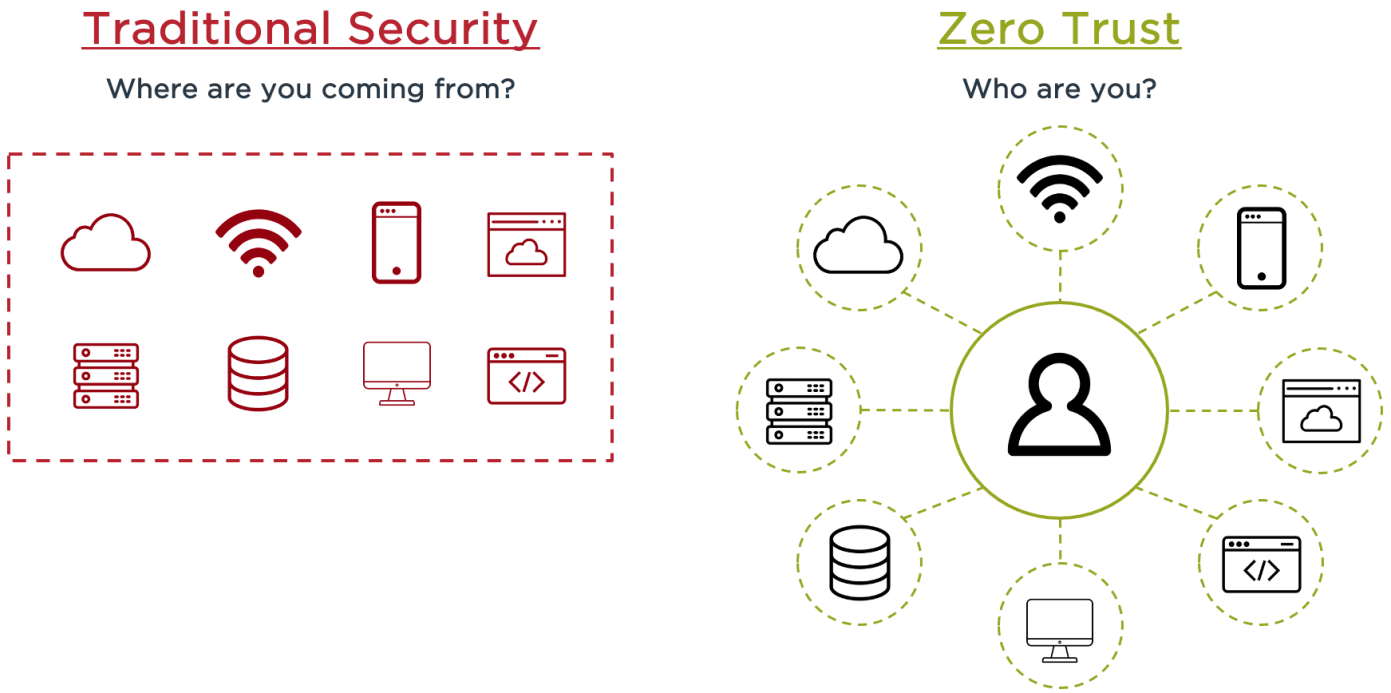


RAZ-LEE iSecurity

Zero Trust Approach

Zero Trust is a strategic approach to cybersecurity that secures an organization by eliminating implicit trust and continuously validating every stage of a digital interaction.

Rooted in the principle of “never trust, always verify,” Zero Trust protect modern environments and enable digital transformation by using strong authentication methods, leveraging network segmentation, preventing lateral movement and simplifying granular, “least access” policies.



RAZ-LEE iSecurity

iSecurity MFA Insights

MFA works based on Persons, who are the owner of one or more users and at the same time they are inside an IP-Group so we can control every movement for every user withing the system.

Our Solution:

- ✓ Enable Secure Sign On.
- ✓ Used to achieve and maintain compliance with leading industry regulations such as PCI-DSS, NIS2, DORA.
- ✓ MFA significantly reduces the risk of system penetration, up to 99%.

RAZ-LEE iSecurity

MFA in iSecurity Implementation

MFA requires beside the standard User/Password, an additional credential:

- ✓ One-Time Password.
- ✓ TOTP tokens - Time Based One-Time Password - RFC 6238.
- ✓ Using iSecurity APP for Apple or Android mobile phones.
- ✓ If the organization has an existing MFA system, it can be used as the additional credential.

Some additional information:

- ✓ TOTP tokens can be generated by the free Google/Microsoft/… Authenticator, or hardware generators.
- ✓ The APP can use: Fingerprint, Face recognition, Pattern, Pin etc.
- ✓ **MFA** of PingID, Duo, Okta are accessed directly to their APP. Other MFAs are connected by a link.

RAZ-LEE iSecurity

Token Generators

We can use ANY token generator that complies with RFC 6238, such as Google Authenticator, Microsoft Authenticator, and others. Usually, they are all free. All you need is a Smartphone.

For those who do not have a smart phone - then can use a hardware devices.

- ✓ Token generators create a six-digit codes.
- ✓ The generated codes changes every 30 seconds.
- ✓ It is known only to your call phone and your IBM i.
- ✓ This knowledge is based on a random 26-characters password.
- ✓ This password is entered once only in both sides.
- ✓ It is usually passed as a QR code, but can also be passed as a Character String.

Optionally, the organization may provide some **Emergency tokens**.

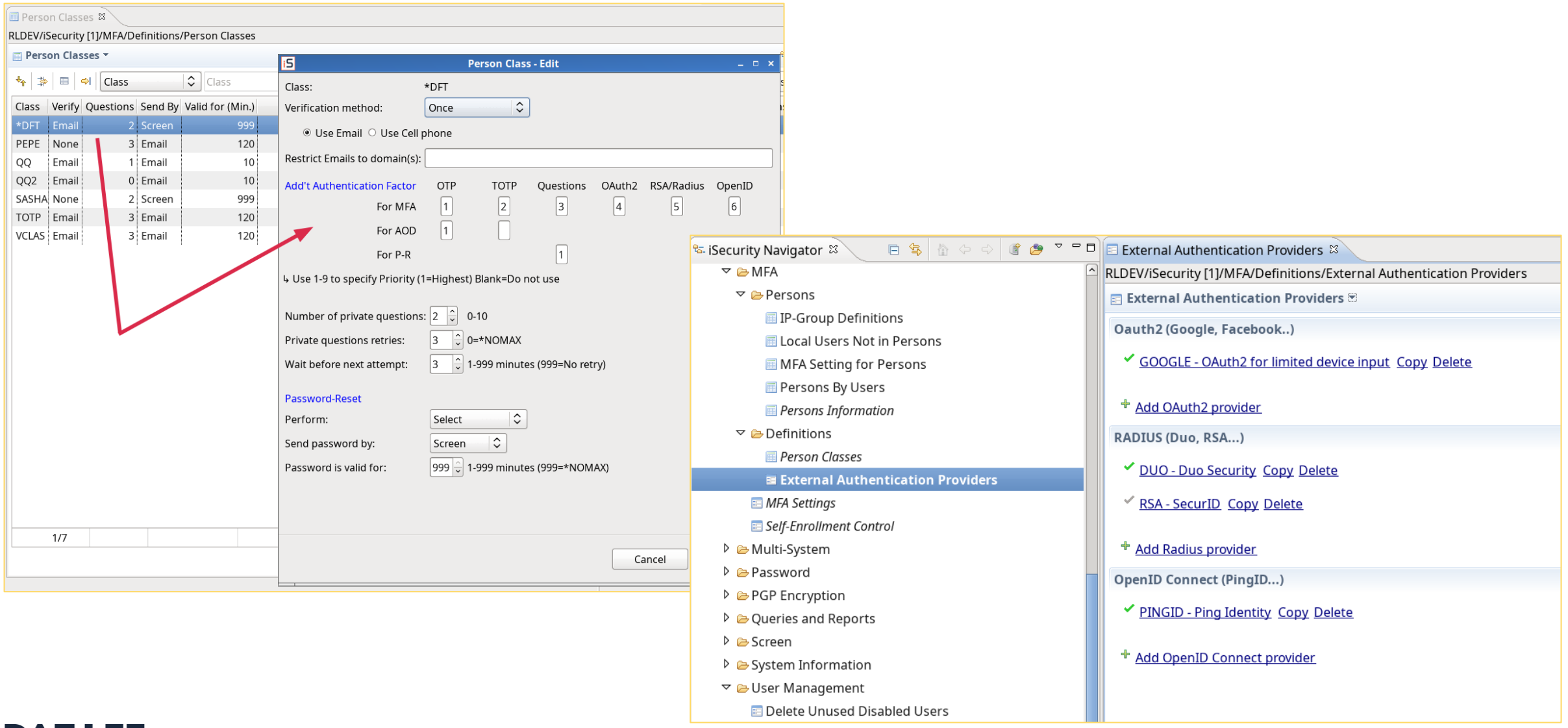
iSecurity
Multi Factor Authentication

Let's see our Product in Action!

The best way to see how it works is a demo with **iSecurity MFA** running on a real environment.

RAZ-LEE

Selecting Authentication Methods



RAZ-LEE iSecurity

Sign On Process

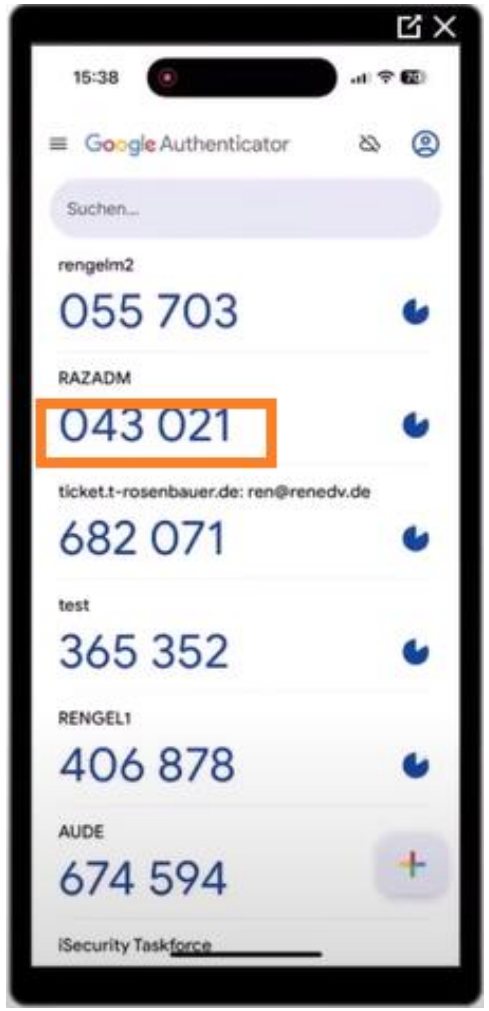
1

```
                    Anmelden
                                  System . . . . . :   RLG
                                  Subsystem . . . . :   QINTER
                                  Bildschirm . . . :   QPADEV0016

Benutzer . . . . . . . . . . . . . RAZADM
Kennwort . . . . . . . . . . . . .
Programm/Prozedur . . . . . . . .
Menü . . . . . . . . . . . . . . .
Aktuelle Bibliothek . . . . . . .
```

2

```
                    Anmeldeinformationen
                                                    System:   RLG
Vorherig
                    Enter MFA Token                 RLG

  Person . . . . . . . RAZADM

  Enter TOTP, or press F7 to request a one time password.

  MFA Token . . . . . .

  F3=Exit    F7=Request a one time password
```

3



4

```
                    Anmeldeinformationen
                                                    System:   RLG
Vorherig
                    Enter MFA Token                 RLG

  Person . . . . . . . RAZADM

  Enter TOTP, or press F7 to request a one time password.

  MFA Token . . . . . . 043021

  F3=Exit    F7=Request a one time password
```

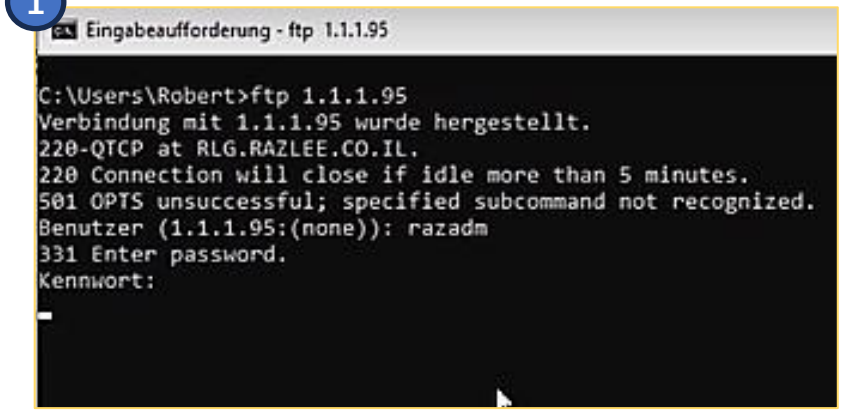
5

```
MAIN                          IBM i-Hauptmenü
                                                System:   RLG
Auswahlmöglichkeiten:

     1. Benutzeraufgaben
     2. Büroaufgaben

     4. Dateien, Bibliotheken und Ordner

     6. Datenfernverarbeitung

     8. Problembehandlung
     9. Menü anzeigen
    10. Unterstützende Informationen - Auswahlmöglichkeiten
    11. IBM i Access-Aufgaben

    90. Abmelden

Auswahl oder Befehl
===> sign

F3=Verlassen    F4=Bedienerführung    F9=Auffinden    F12=Abbrechen
F13=Unterstützende Informationen    F23=Anfangsmenü festlegen
(C) COPYRIGHT IBM CORP. 1980, 2018.
MA  B                                           20/011
```

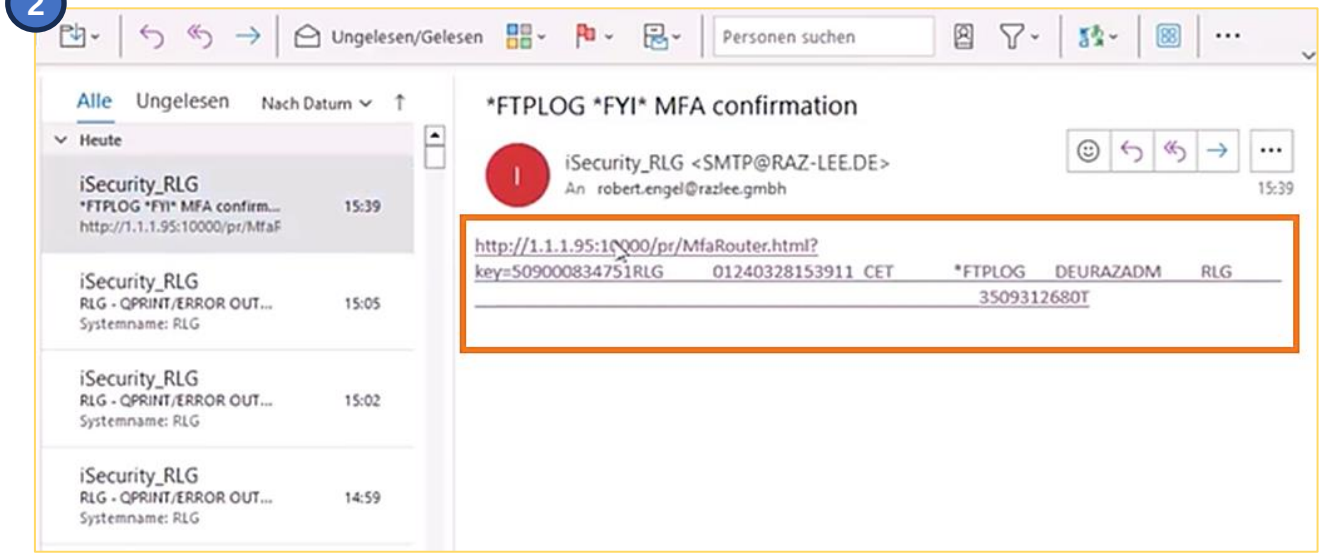
RAZ-LEE iSecurity

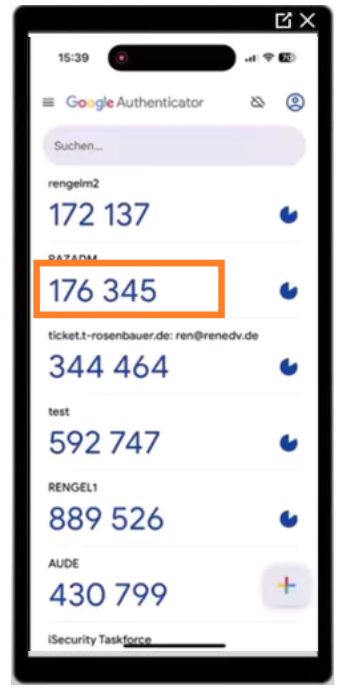
FTP Sign On Process

1



2





3

4

RAZ-LEE iSecurity

iSecurity
Multi Factor Authentication

Advantages on our Solution

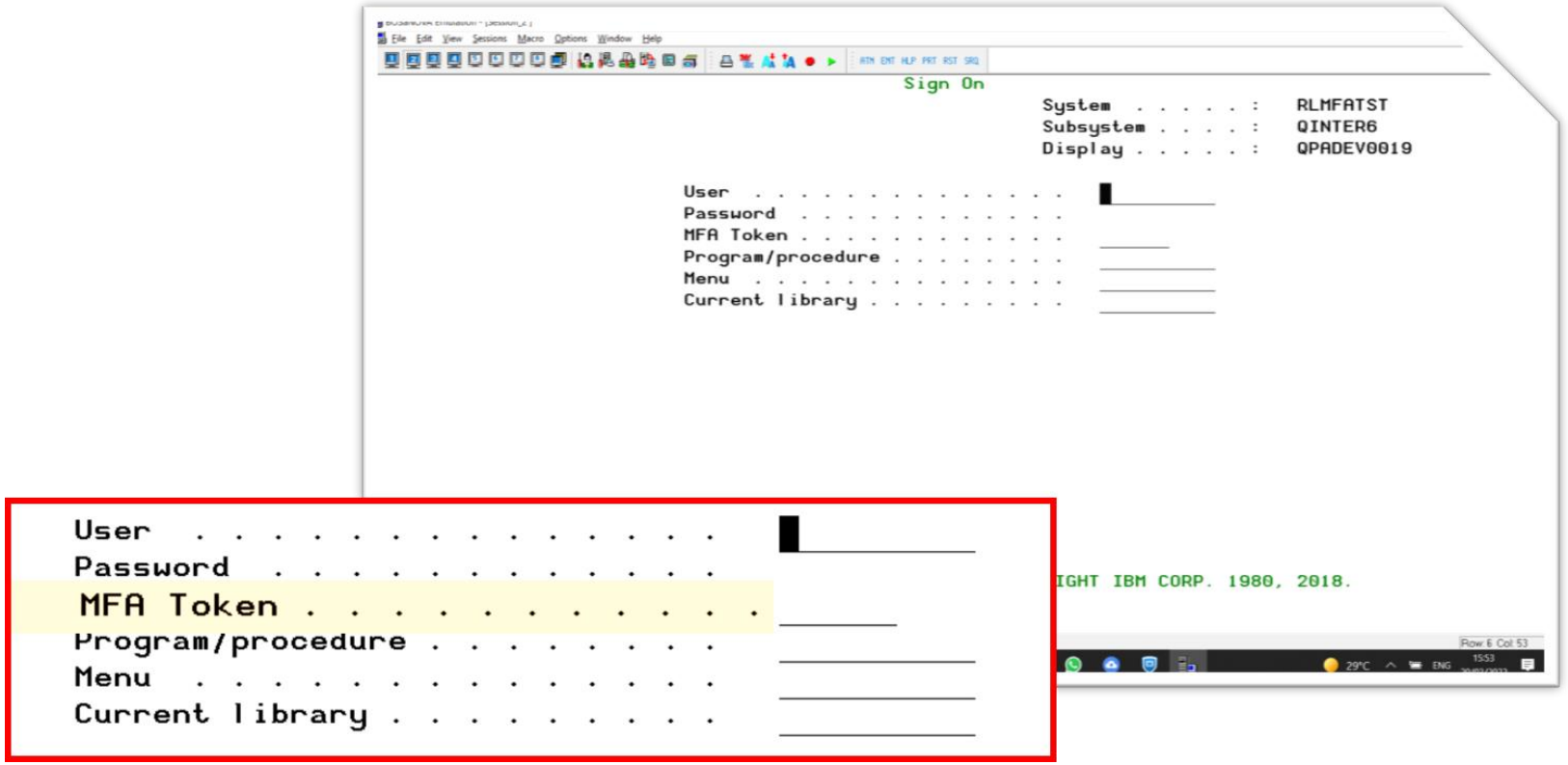
iSecurity MFA can control every movement for every user withing the system.

RAZ-LEE

One Step Authentication

Single Step

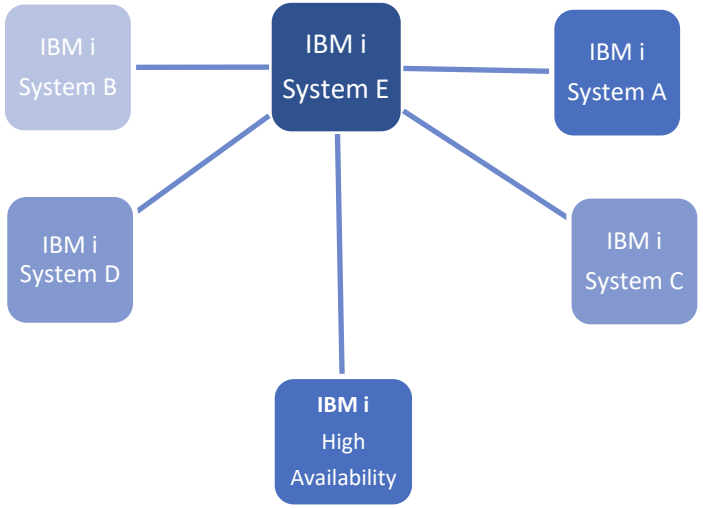
Single Step Authentication is considered safer. **iSecurity MFA** enables you to modify the IBM i standard Sign On screen by adding the MFA Token entry field, following the regular password



RAZ-LEE iSecurity

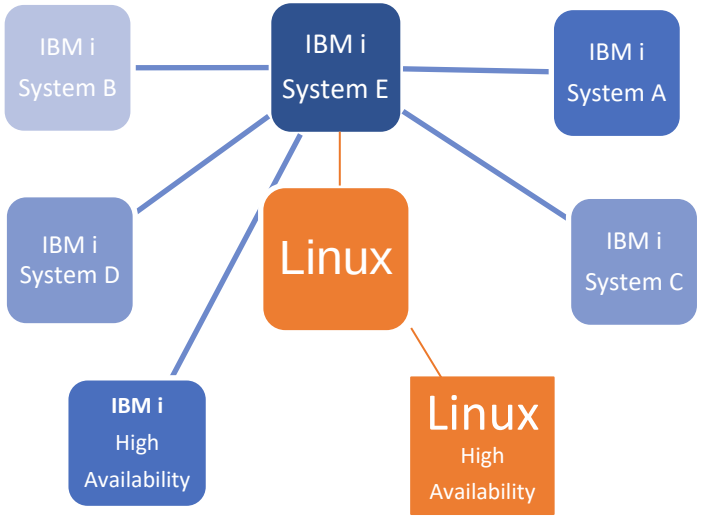
Simplicity

iSecurity MFA/Password-Reset/Authority On Demand



- ✓ Completely Native to the IBM I
- ✓ It installs and activates in minutes
- ✓ No need of additional hardware server
- ✓ No special Smartphone application is needed
- ✓ No special PC application is needed
- ✓ No knowledge of other OS is needed

Others' approach



- × Additional Hardware
- × Additional Software
- × Second Operating System
- × High Complexity

RAZ-LEE iSecurity

MFA Building Blocks – Person

Person

We are all human beings. We do not wish to get verified again and again. This is why we use the term, Person. This is why we verify Person and not User Profile.

Each Person may have multiple user profiles on multiple systems. Once a Person signs by one of his user profiles, and has been verified by **MFA** as working from a certain IP, he is not bothered again when he signs from the same IP to another session on this or other systems with a user profile that belongs to him.

This verification may be limited by time and includes Regular Sign On, as well as TCP services such as FTP, ODBC, REXEC, IFS share, etc.

RAZ-LEE iSecurity

MFA Building Blocks - IP Group

IP Group

The regular IP Addresses from which a Person signs on can be grouped in an IP Group, e.g. one or more offices and home addresses.

With **MFA**, you can decide what the system should do when a person signs on from within or from outside of the IP Group. You can decide to use **MFA** only when signing on from the outside, or request **MFA** when signing on from within, and reject other attempts.

This behavior can be set differently for regular Sign On, FTP, ODBC, REXEC, IFS share etc.

RAZ-LEE iSecurity

Persons and Locations

Now we talk about the combination of Person + IP group, this is extremely important because we can block or allow a person to enter the system depending on his location, so we totally ensure not only that the person is who she says she is, also we know where that person is logging in from.

John

- New York
- Atlanta (2 User Profiles)
- Tel Aviv
- Home

MFA Required Inside

Otherwise Rejected

Nataly

- New York (3 User Profiles)
- Atlanta

MFA Not Required Inside

MFA Required Outside

Matthew

- Tel Aviv
- Home

MFA Not Required Inside

Otherwise Rejected

RAZ-LEE iSecurity

iSecurity Multi-Factor Authentication Advantages

- ✓ **TCP/IP exit points support:** Our solution provides authentication not only to the standard login, also to TCP/IP servers (exit points).
- ✓ **Additional flexibility:** Based on the IP address from which a user accesses the IBM i. Based on predefined IP Groups (Location. Ranges) users can be rejected / require or not require authentication within the IP group.
- ✓ **iSecurity MFA is native to the IBM i:** Only uses standard applications on it and on smart phones. No need for additional hardware server, no special apps on phones and PCs.
- ✓ **Simplicity for 'Persons':** Users may have multiple profiles to access different systems. **iSecurity MFA** introduces the concept of a person rather than based on profiles. When a person is authenticated once (including the IP group), users can access using any of their user profiles.
- ✓ **Freedom of Authentication Method:** Users of Radius, Qauth2, OpenID (PingID) can get authenticated by one of these apps, **MFA** will continue having these apps in control of the users, eliminating the need for additional authentication.

RAZ-LEE iSecurity

RAZ-LEE

Contact us About our Products

Sales Representatives

sales@razlee.com

Visit Our Website

www.razlee.com

iSecurity

Multi Factor Authentication