ICE/PSWD - Your z/OS Image Sentry

An Integrity Controls Environment (ICE) Application

The 2017 Data Breach Investigations Report* (DBIR) notes that 81% of hacking-related system breaches leveraged either stolen logon credentials and/or weak, sometimes even guessable, user passwords.

ICE/PSWD Answers the Challenge

With this shocking statistic in mind, we designed and developed ICE/PSWD to answer the password integrity challenge. Our goal is to provide a way forward for implementing the DBIR Best Practice recommendations, within the z/OS Mainframe Community.

The First DBIR Challenge – "Make people your first line of defense".

Using simple Parmlib constructs, ICE/PSWD makes it easy to adopt practices commonly experienced on the WWW when transacting with digital commerce sites/online services such as your bank

• • • • • • • •

The Second DBIR Challenge – "Encourage stronger passwords".

This is easy to say, but harder to do. The z/OS Security systems do support stronger password constructs in the form of syntax format rules but often don't get an opportunity to enforce them. It's possible to define more than

• • • • • • • •

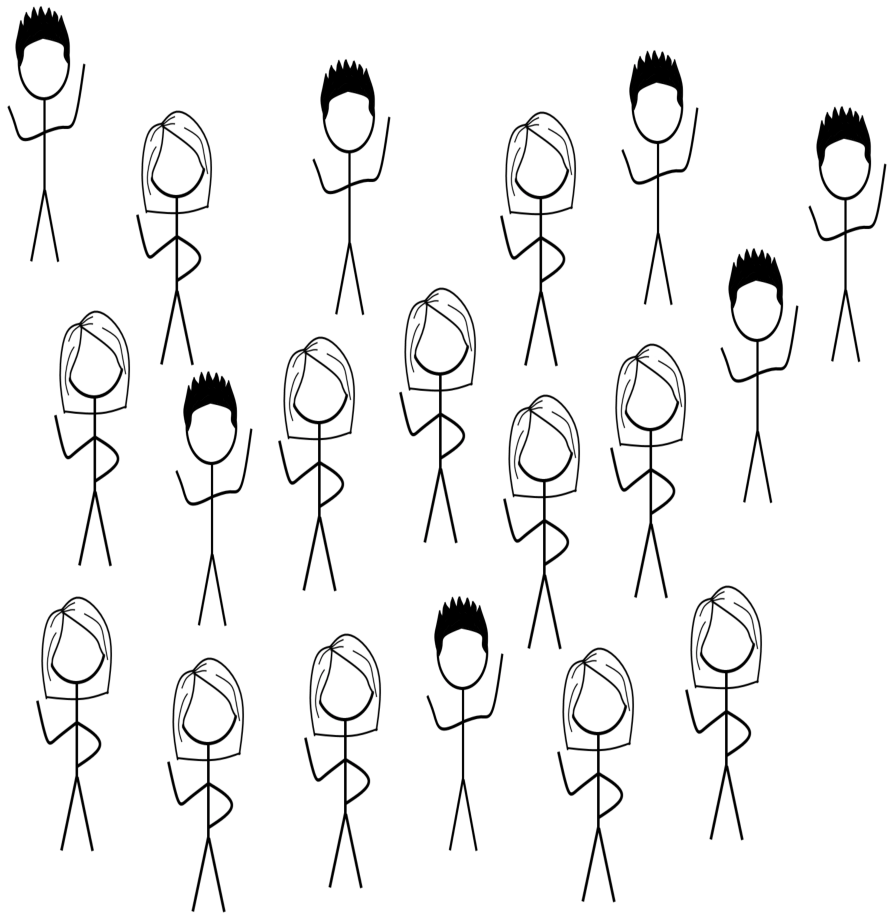
The Third DBIR Challenge – "Use multi-factor authentication".

There is no doubt, multi-factor authentication will add integrity to the strength of credentials used to access any system, including z/OS. But once you're in, you're in. If you've hacked in with a stolen credential, one of your first or

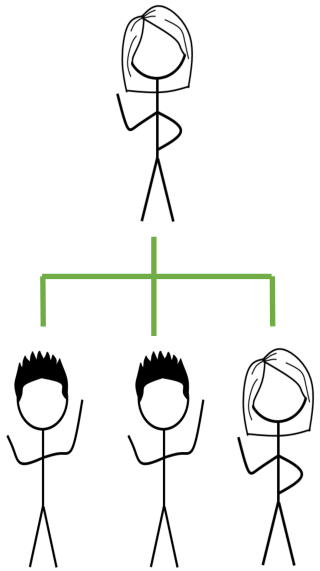
http://www.newera.com/INFO/ICE-PSWD.pdf

* Verizon's 2017 Data Breach Investigations Report

There are Three Possible System Credentials



Permitted but not Privileged



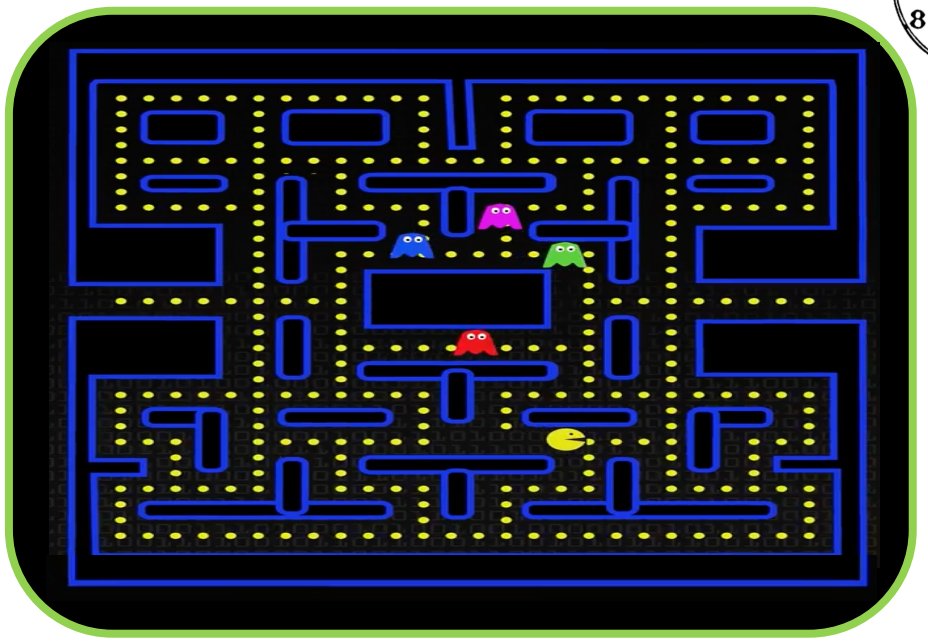
Privileged

Compromised

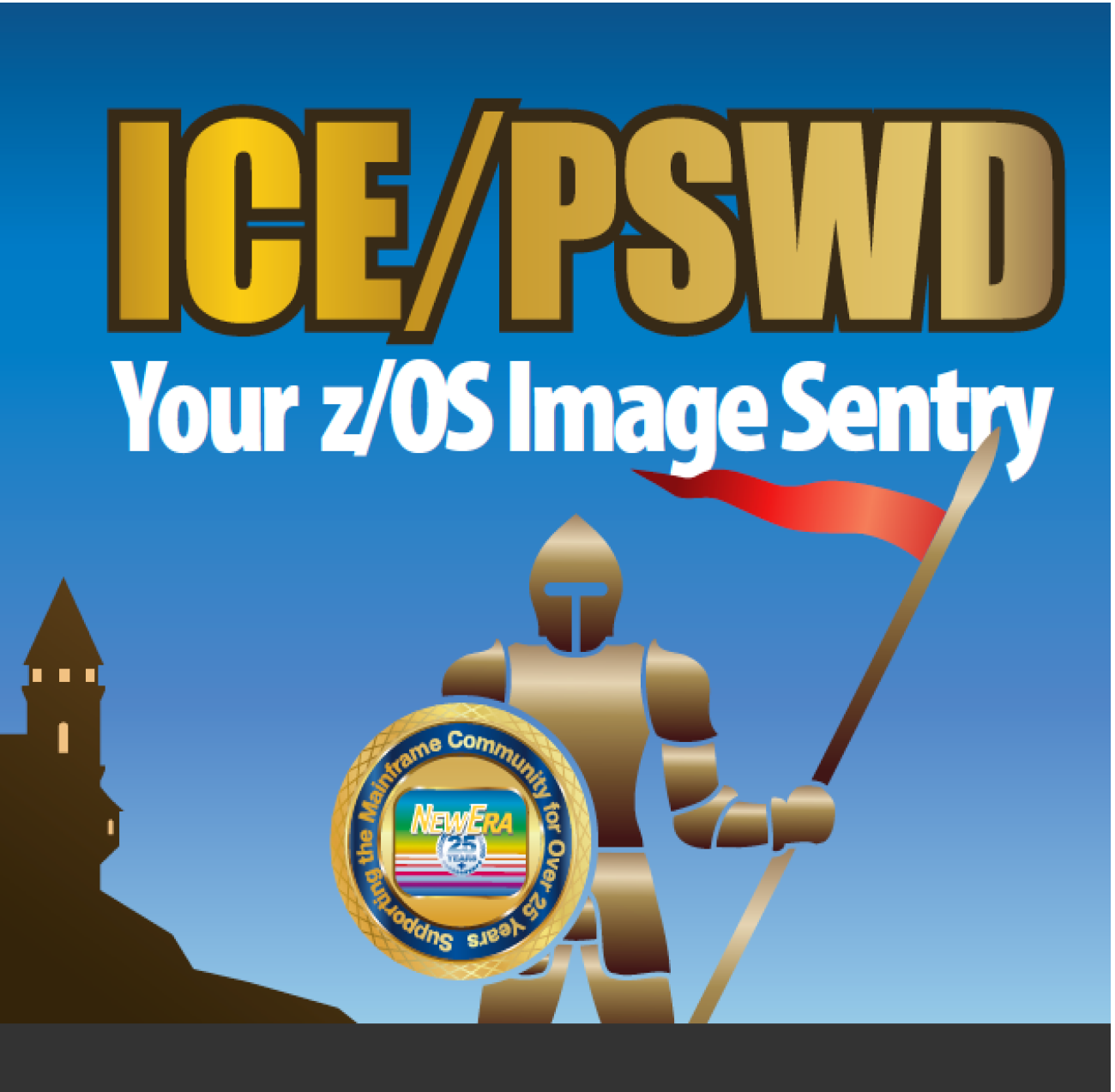
A Privileged User is one that is able to:

- Change Security Controls
- Access/Copy Sensitive Data
- Change System Configuration Settings
- Circumvent Event Monitoring and Detection

When Credentials are Compromised:



Why a z/OS Image Sentry?



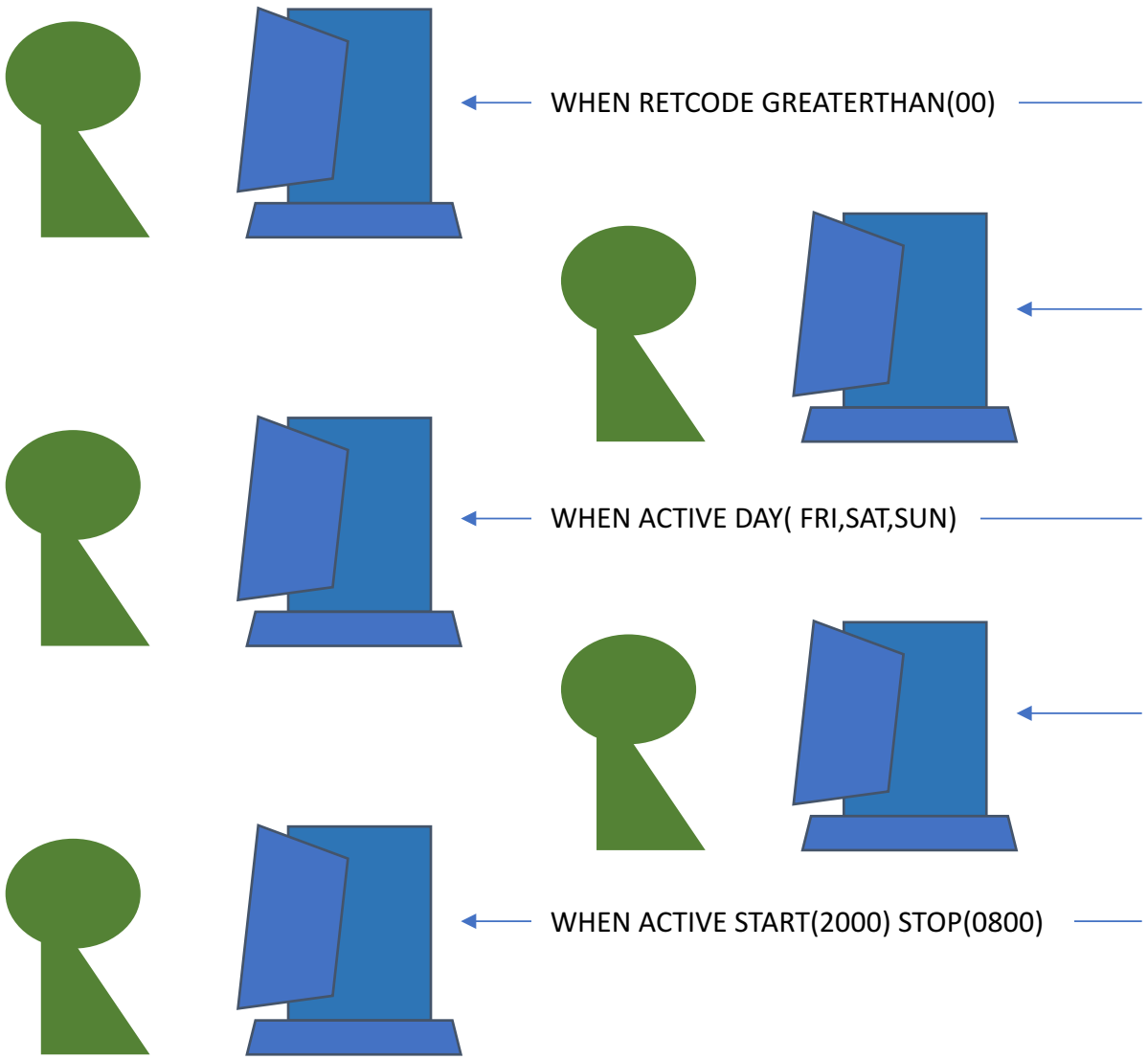
For most large organizations, credential theft is an everyday occurrence. (IBM Systems Media)

We consider it self-evident that z/OS System Integrity is enriched by the inclusion of the user as an active participant in the overall z/OS mainframe Security Paradigm. Following this webcast, we believe you will also.

Consider this: in real time, the Only Person who can ACTUALLY know if YOUR logon credential is being used legitimately is YOU! Not a SIEM, not the Help Desk, certainly not an SMF record of any type. Just YOU and YOU alone!

Know now, that organizations can enlist their user communities in a common sense defense of the z/OS mainframe perimeter by providing near real-time services that allow them to be vigilant over the misuse of their credentials, privileged or not, when used for system logon and/or Password or Passphrase reset.

How do Your Users Benefit?



Your user community becomes part of the 'Security Team' benefiting in three specific ways:

First, notification of credential use gives your users confidence that their integrity and the integrity of the system has not been undermined by credential theft.

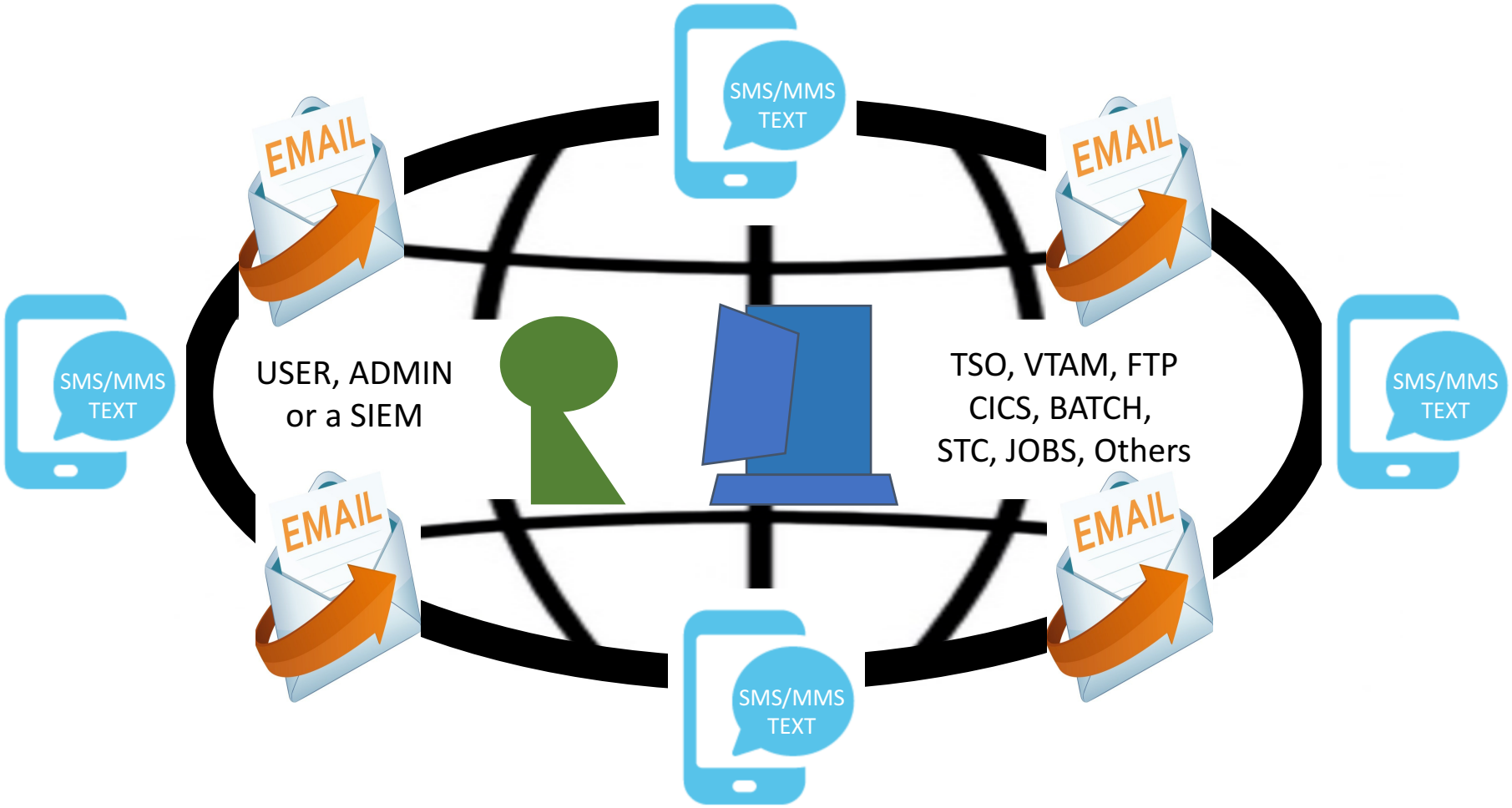
Second, notification of password/phrase reset request/attempt provides to users additional assurance that overall integrity remains intact and that they have not been 'Locked Out'.

These notices are easily configured to occur only during 'Watchful Periods' or in response to a 'Watchful Condition' - i.e. a return code.

Third, impending expiration notices assure users an ample window-of-time for considering stronger passwords/phrases, perhaps when conforming to new practices or more demanding 'Best Practices'.

How does ICE/PSWD Prevent ‘Flooding’?

‘Flooding’ is a condition that would exist if – Email, TEXT, SIEM – were sent with each – Logon, Reset, Expiration – event. Not a good idea!
ICE/PSWD deals with this issue by supporting the creation of ‘Watchful Periods’ and ‘Watchful Conditions’.



```
ICE 15.0 - Logon Notice Rule Details
Selected NoticeId PROBI1   /. Allow Updates

TO:           /. PRR@NEWERA.COM
Copy:         /. SYSSEC@NEWERA.COM
Alias:        /. HELPER BEE
Subject:      /. YOU JUST LOGGED ON
Inactive On:  /. VEGAS01,VEGAS02
Active Time:  /. STM(2000) ETM(0800)
Active Day:   /. DAYS(SAT,SUN)
Active RC:    /. GREATERTHAN(00)
SIEMRoute:    ..
From:         /. SUPPORT@NEWERA.COM
Domain:       ..
EMailDebug:   /. ON    Journal: /. ON    NoMail: ..
```

Creating/Defining
'Watchful Periods' and 'Watchful Conditions'.

```
ICE 15.0 - Logon Notice Rule Details
Selected NoticeId PROBI1   /. Allow Updates

TO:           /. PRR@NEWERA.COM
Copy:         /. SYSSEC@NEWERA.COM
Alias:        /. HELPER BEE
Subject:      /. YOU JUST LOGGED ON
Inactive On:  /. VEGAS01,VEGAS02
Active Time:  /. STM(2000) ETM(0800)
Active Day:   /. DAYS(SAT,SUN)
Active RC:    /. GREATERTHAN(00)
SIEMRoute:    ..
From:         /. SUPPORT@NEWERA.COM
Domain:       ..
EMailDebug:   /. ON    Journal: /. ON    NoMail: ..
```

Creating/Defining
'Watchful Periods' and 'Watchful Conditions'.

Typical Email and/or SMS/MMS Message Content

```
-SRC: SYSLOGON(TOKTSO  )---THE CONTROL EDITOR---------- VerifySuccess -
SYSPLX:ADCDPL   SYSNM:ADCD22B  USRID:********    TM:15:20:18 DT:03/07/18
-VERIFY(X): HELPER BEE----------------------RC: 00--------------------
```

Creating/Defining
'Watchful Periods' and 'Watchful Conditions'.


```
ICE 15.0 - Logon Notice Rule Details
Selected NoticeId PROBI1   /. Allow Updates

TO:           /. PRR@NEWERA.COM
Copy:
Alias:
Subject:
Inactive On:
Active Time:
Active Day:
Active RC:
SIEMRoute:
From:
Domain:
EMailDebug:
```

```
ICE 15.0 - Password Change Notice Rules
Selected NoticeId PROBI1   /. Allow Updates

To:           /. PRR
Copy:         /. GHB
Alias:        /. BANDIT
Subject:      /. YOUR PASSWORD CHANGED
Inactive On:  ..
Active Time:  /. STD(180330)
Active Day:   ..
SIEMRoute:    /. 222.222.222.222
MsgBody:      /. IF YOU SEE SOMETHING REPORT IT
From:         /. SUPPORT
Domain:       /. @NEWERA.COM
EMailDebug:   /. ON   Journal: /. ON   NoMail: ..
```

Domain,
what is it?

Creating/Defining
'Watchful Periods' and 'Watchful Conditions'.


```
ICE 15.0 - Logon Notice Rule Details
Selected NoticeId PROBI1   /. Allow Updates

TO:              /. PRR@NEWERA.COM
Copy:
Alias:
Subject:
Inactive On:
Active Time:
Active Day:
Active RC:
SIEMRoute:
From:
Domain:
EMailDebug:
```

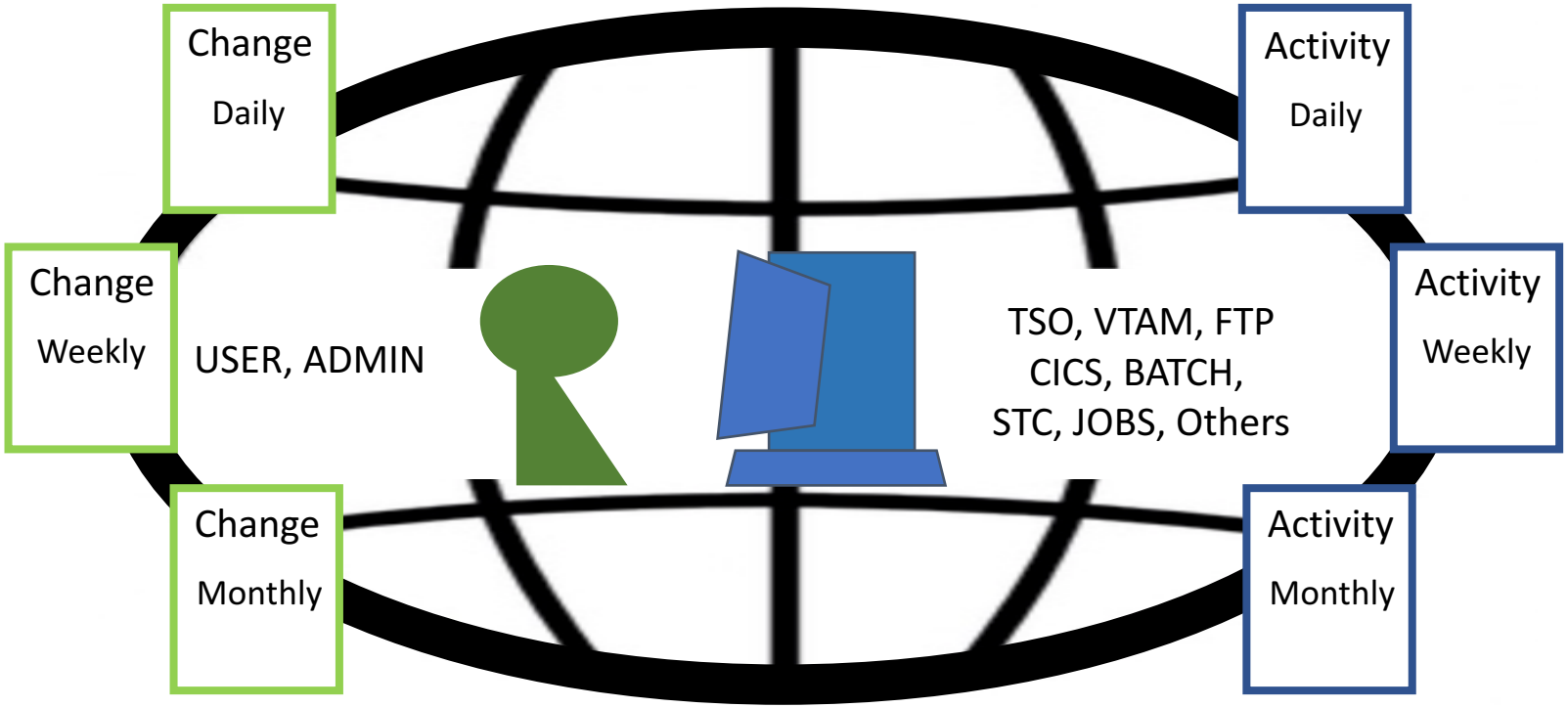
```
ICE 15.0 - Password Change Notice Rules
Selected NoticeId PROBI1   /. Allow Updates

To:              /. PRR
Copy:
Alias:
Subject:
Inactive On:
Active Time:
Active Day:
SIEMRoute:
MsgBody:
From:
Domain:
EMailDebug:
```

Domain,
what is it?

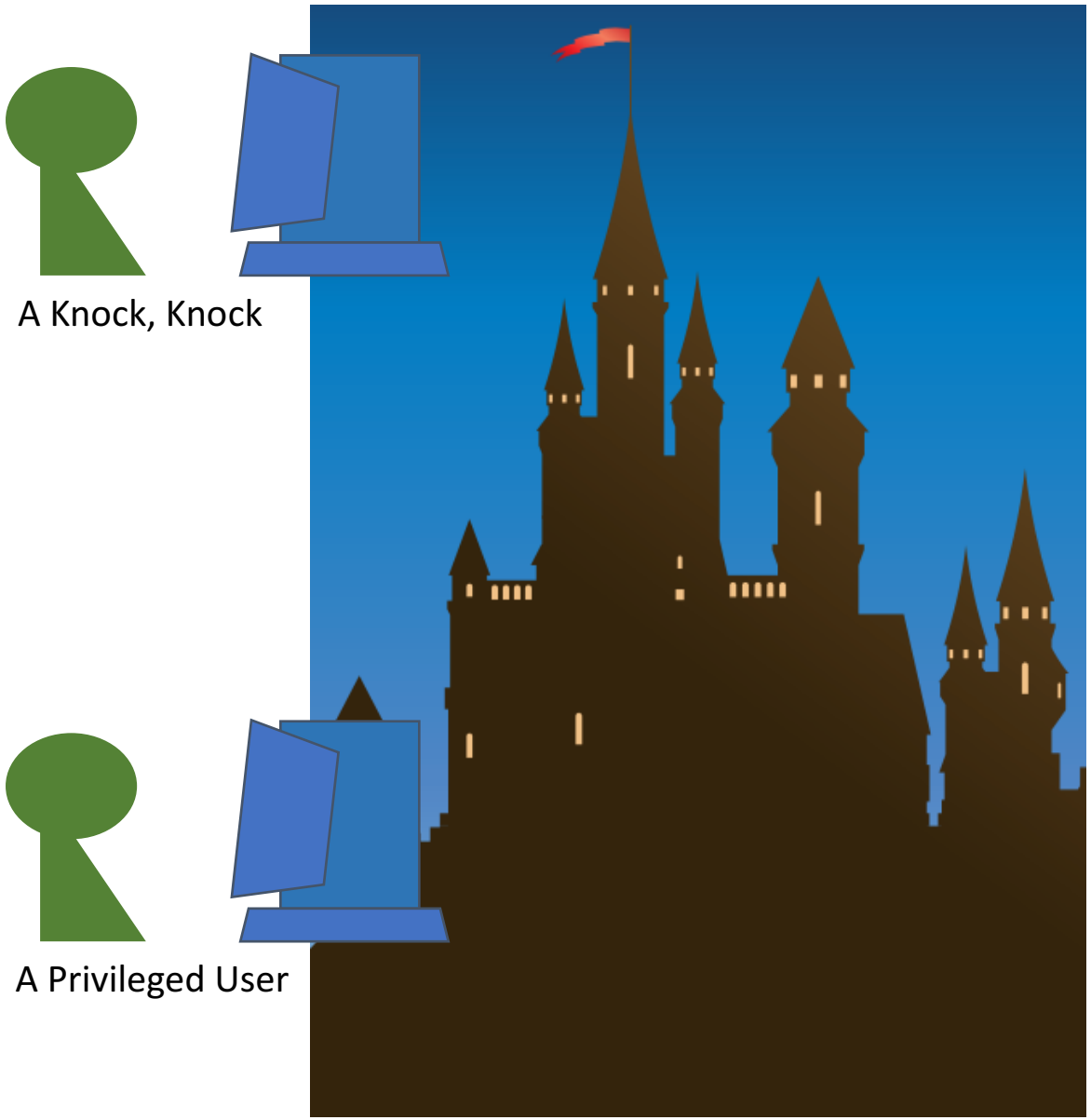
```
ICE 15.0 - Expire Notice Rule Details
Selected NoticeId PROBI1   -. Allow Updates

To:              /. PRR@NEWERA.COM
Copy:            /. JIM@NEWERA.COM
Alias:           /. UNKNOWN CARBON ENTITY
Subject:         /. EXPIRATION_NOTICE
Intervals:       /. 0,1,2,3,5,10
From:            /. PAT@NEWERA.COM
Domain:          ..
EMailDebug:      /. ON    Journal: ..     NoMail: ..

   Updates Not Allowed Enter 'R' > .. > Press Return
```

How does ICE/PSWD Prevent ‘Flooding’?

‘Flooding’ is a condition that would exist if – Email, TEXT, SIEM – were sent with each – Logon, Reset, Expiration – event. Not a good idea!
ICE/PSWD deals with this issue by supporting the creation of ‘Watchful Periods’ and ‘Watchful Conditions’.



Who's there knocking on the Door?



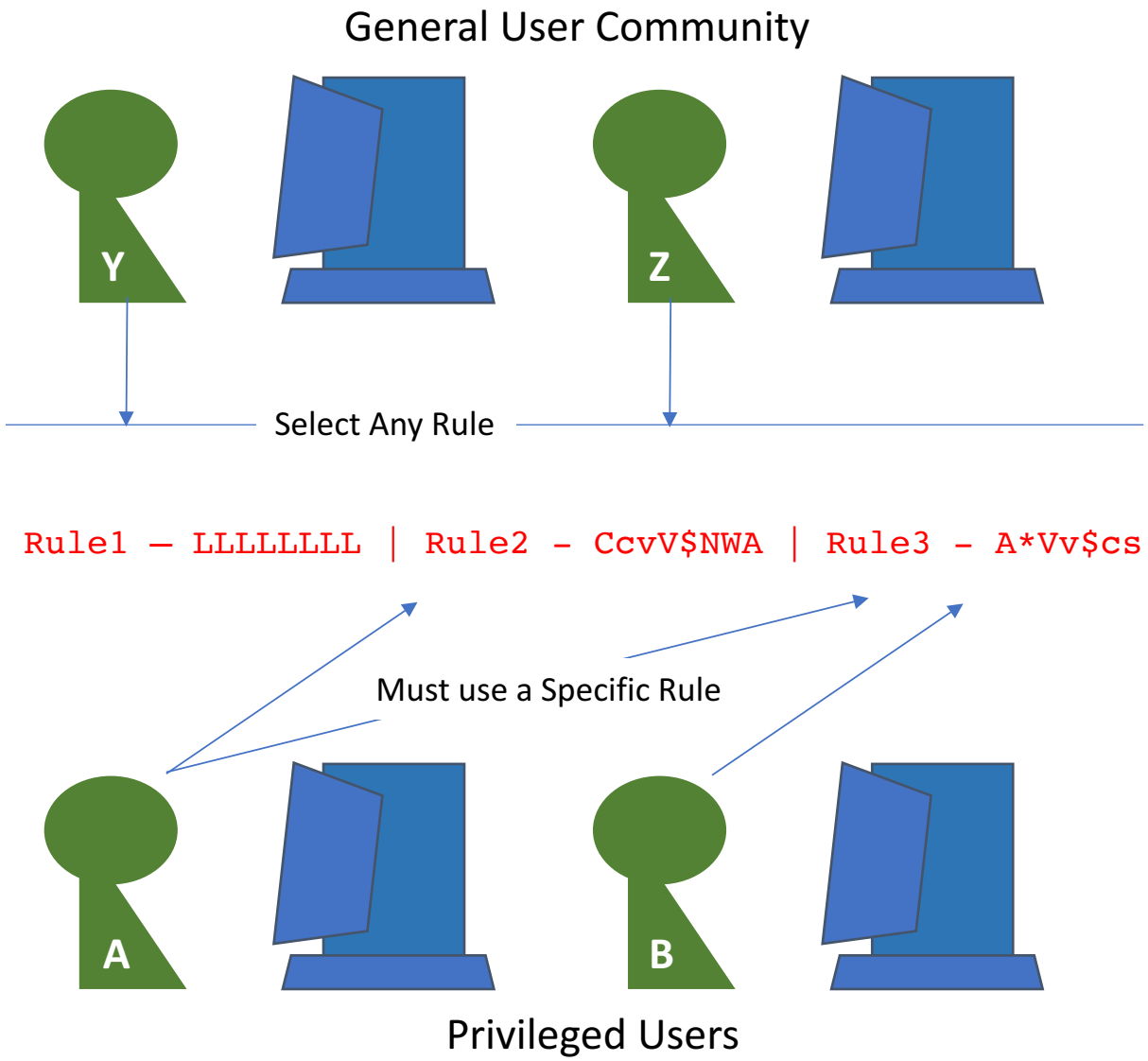
IBM Security Server RACF stepped up its game by supporting PASSWORDPREPROMPT. This optional control can deny potential unauthorized users access to valuable logon panel content, visible and/or hidden. But logon attempts using unknown/invalid UserIds are still a common occurrence.

A single Control Card added to ICE/PSWD prompts your z/OS Sentry to report these attempts to SECURITY STAFF via email/TEXT or directly to a designated SIEM.

Privileged logons, users with a privileged RACF attribute - OPERATIONS, SPECIAL, AUDITOR, ROAUDITOR, REVOKED – or those on a 'Watch List' are always of interest.

Again, a single Control Card added to ICE/PSWD directs your z/OS Sentry to report these logons to SECURITY STAFF via email/TEXT or directly to a designated SIEM.

How Does Format Binding Work?

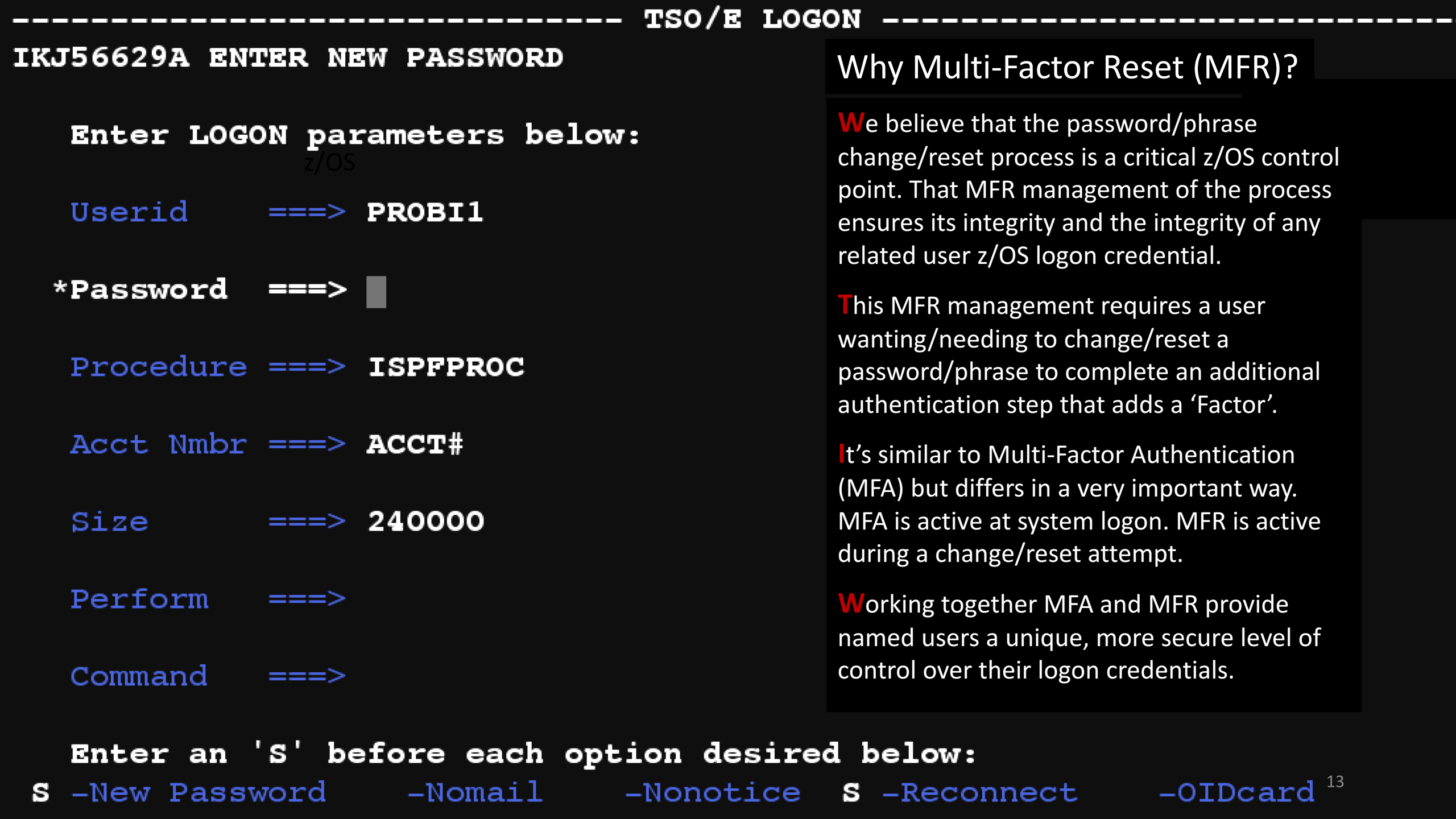


IBM Security Server RACF provides for eight syntax format rules. These rules can vary considerably in terms of complexity. Users can choose which available rule they will conform to during password/passphrase reset process.

Some users may select a complex rule, but others might succumb to 'Human Nature' and select the simplest; perhaps because it's easier to remember.

This flexibility makes it difficult to implement a requirement for more complexity as doing so would impact the entire user community.

Format binding overcomes this "Catch 22" by allowing your security team to assign more complex formats on a user by user basis to privileged users, while allowing general users to select formats as they have been trained.



Why Multi-Factor Reset (MFR)?

We believe that the password/phrase change/reset process is a critical z/OS control point. That MFR management of the process ensures its integrity and the integrity of any related user z/OS logon credential.

This MFR management requires a user wanting/needing to change/reset a password/phrase to complete an additional authentication step that adds a 'Factor'.

It's similar to Multi-Factor Authentication (MFA) but differs in a very important way. MFA is active at system logon. MFR is active during a change/reset attempt.

Working together MFA and MFR provide named users a unique, more secure level of control over their logon credentials.

What is Multi-Factor Reset (MFR)?

This password/phrase Change/Reset Control requires a user who wants to change/reset a password/phrase to complete an additional authentication step that adds a factor.

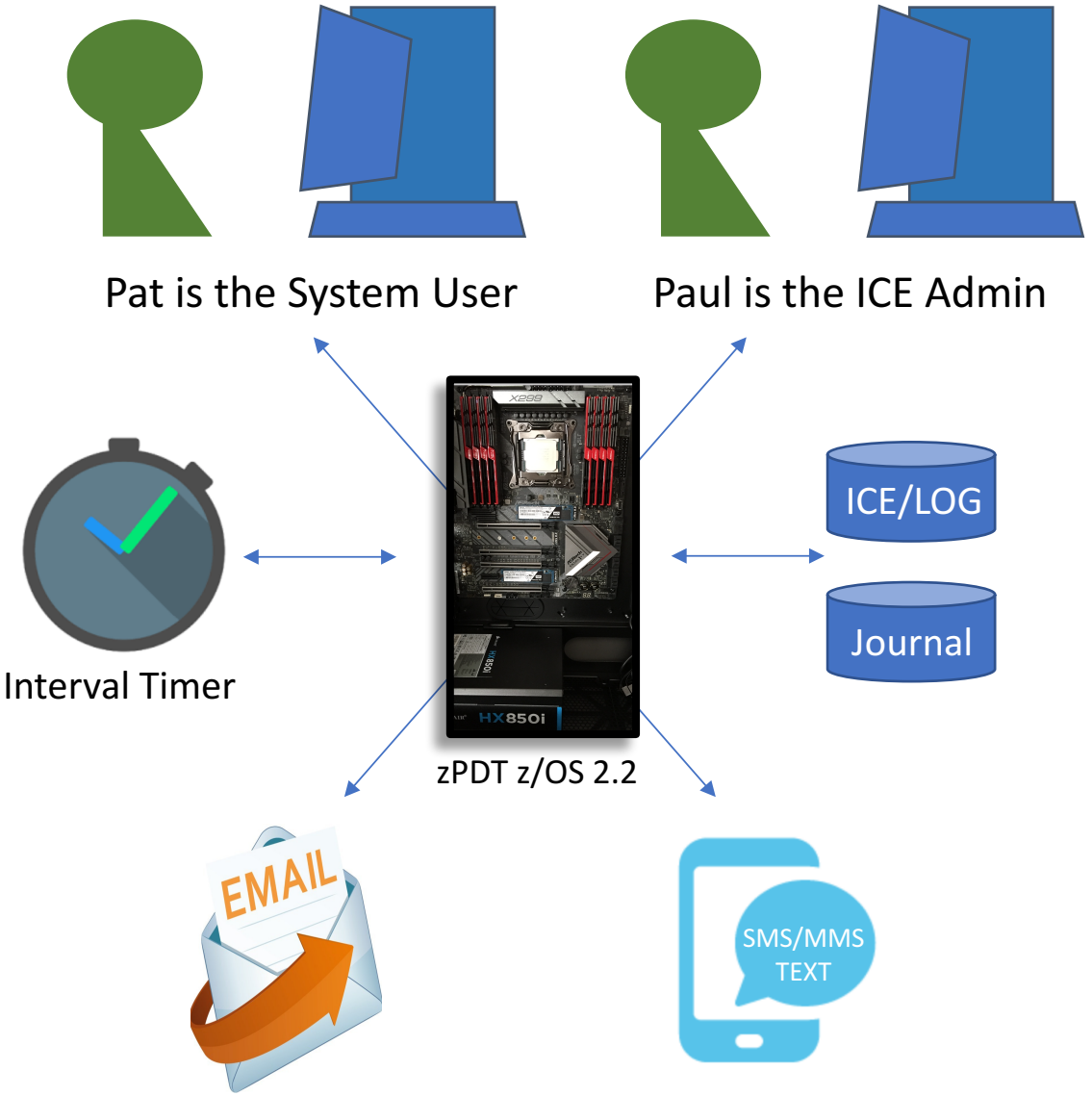
First, the user would attempt a normal logon and password/phrase reset.

Next, ICE/PSWD generates a time-sensitive, One-Time Password (OTP) value that is sent to the user via email or SMS/MMS text.

In an optional accompanying message, the user is instructed to return to the originating system, within the specific time window, to complete the requested reset.

To finish the reset, the user needs to enter both the current password/phrase and the OTP value as a new password/phrase value (with confirmation). If this is completed successfully, the reset will be honored.

ICE/PSWD Product Demonstration



Agenda:

- Invalid or unknown UserId Notification
- System Logon Notification
- Password/Phrase Change/Reset Notification
- Password/Phrase Expiration Notification
- Multi-Factor Password/Phrase Change/Reset
- Setting up a Format Binding Rule
- A Brief Look at a User Service Account and
- User Service Account Reporting

Links:

- http://www.newera.com/INFO/ICE-PSWD.pdf
- http://www.newera-info.com/Docs.html

A User Service Account

.. UserLogons .. UserPswCng .. PswdExpire .. FormatRule .. OTPControl
.. 2018/03/07 .. 2018/03/06
PROBI1 PROBI1

A Service Account is a collection Logon, Password Change and Expiration notification Rules, Password Format Bindings and Multi-Factor Reset Controls and users Logged/Journaled Activity Event Access and Reporting.

Users assigned a Service Account may or may not be given access to it. If access is allowed users may or may not self-manage their account gaining access to their Activity Event Worksheets for viewing and/or for updating their background reporting and report distribution options.

The Administrator assigns, oversees and grant access to the Service Accounts setting user and global defaults.

--------Event Worksheets--------

---ICE/PSWD--- ---ICE/TCE---

.. UserLogons		.. ManageEdit	
.. 2	281	.. 0	10
.. UserPswCng		.. CmmdUpdate	
.. 0	0	.. 0	1
.. PswdExpire		.. SubmitJobs	
.. 0	0	.. 0	0
.. FormatRule		.. OtherEvent	
.. 0	0	.. 0	0
.. OTPControl		.. EveryEvent	
.. 0	0	.. 2	292

------User Report Cycle /. Allow----

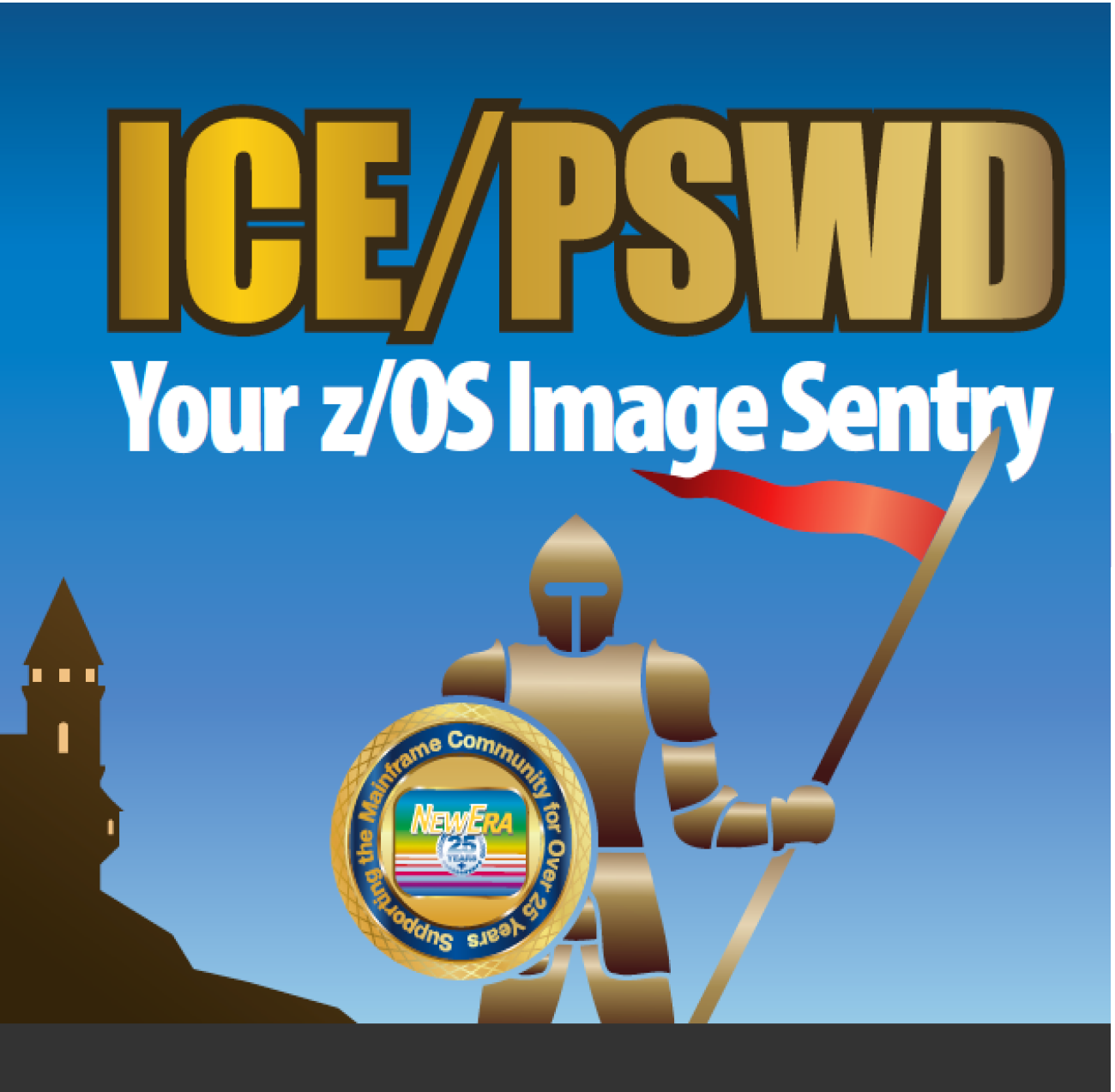
/. Active /. Event /. Chngs /. New

/. Day - 01 10 - 24 Hour Interval
24hh mm 1|2|4|6|8|12|24
.. Wks - 02 20 - SUN,MON,TUE
24hh mm SUN,MON,TUE,Etc.
.. Mth - 03 33 - 1,2
24hh mm Day:1,2,9,25,EOM
/. Pre PRR
Dom @NEWERA
/. Copy NoticeId Reports to Admin

.. Your PSWD Access Token .. Update Service Account

Please Complete the Survey.

http://survey.constantcontact.com/survey/a07ef6172r5je63qzm8/start



ICE/PSWD Survey

1.

Thank you for taking the time to complete our one question survey. All responses will be anonymous. Use the Comment box for comments or recommended enhancements. Click FINISH to send your responses.

Please rate the proposed functions in order of importance to you with 5 being most important through 1 being lease important.

(1 = Least)

-- System Logon Notification

-- Password/phrase Change Notification

-- Multi-Factor Reset Notification - Adding a "Factor"

-- Password/phrase Expiry Notification

-- RACF Password/phrase Format Binding

Comment:

500 characters left.

Finish

Thank you. Remember Only You Know for Certain.

Recent Download

Dear Paul,

Your Apple ID, prr@newera.com, was just used to download Amazon Kindle from the iTunes Store on a computer or device that had not previously been associated with that Apple ID. You may also be receiving this email if you reset your password since your last purchase.

If you initiated this download, you can disregard this email. It was only sent to alert you in case you did not initiate the download yourself.

If you did not initiate this download, we recommend that you go to iforgot.apple.com to change your password, then see Apple ID: Security and your Apple ID for further assistance.

We noticed a recent login for your account @pamelarobichaux.

Device	Safari on Mac
Location*	Morgan Hill, CA

*Location is approximate based on the login's IP address.

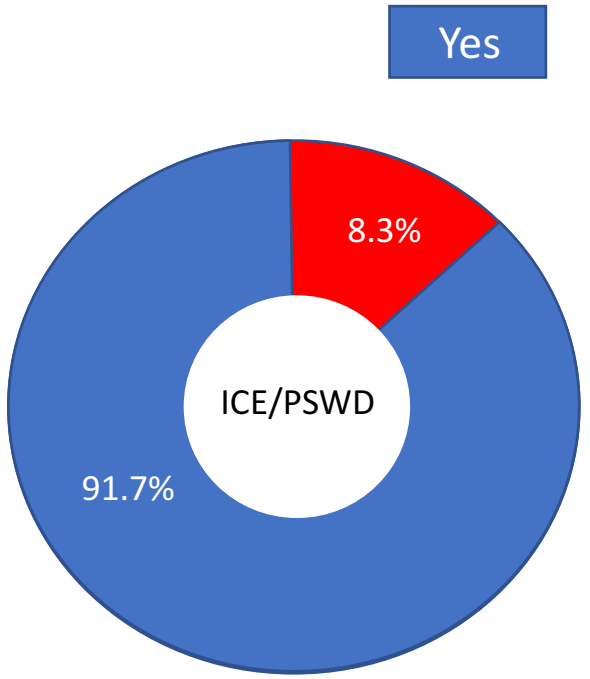
If this was you:

Great! There's nothing else you need to do.

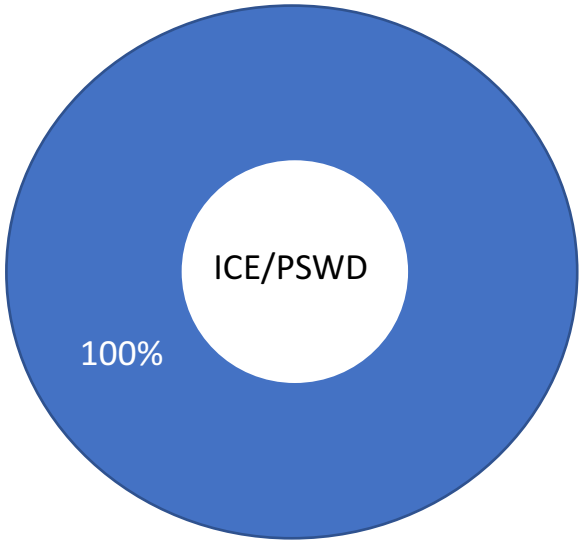
If this wasn't you:

Your account may have been compromised and you should take a few steps to make sure your account is secure. To start, reset your password now.

Do you feel that these enhancements could help you to improve your security culture?



Guide Share Europe (GSE UK) Security Working Group (12)
Attendee written Survey responses, February 8, 2018.

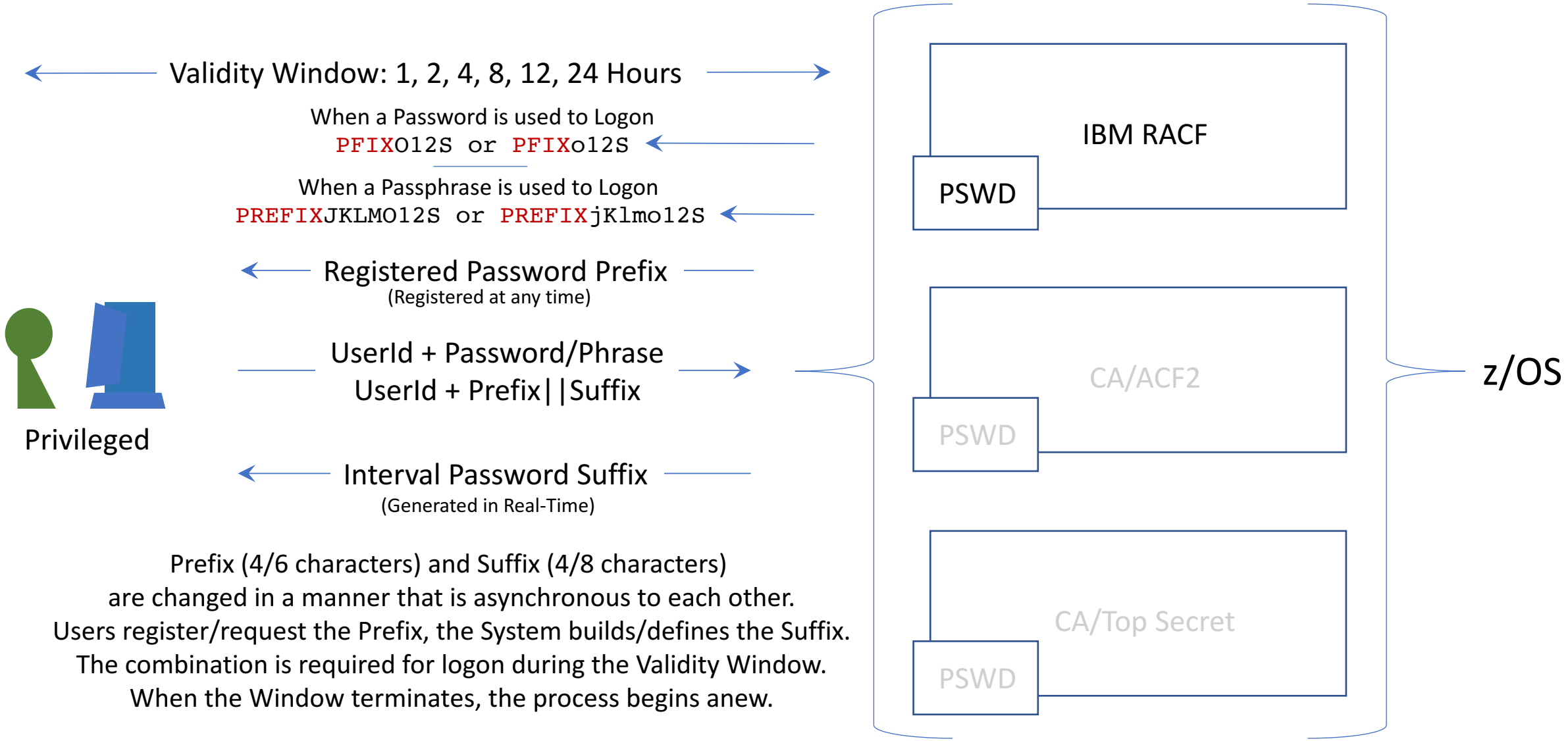


ICE/PSWD Introduction Web Cast
Attendance 22 of which 10 completed The Post Web Survey
As of, March 7, 2018.

Maybe helpful towards GDPR or PCI Compliance?

Multi-Factor Logon (MFL)

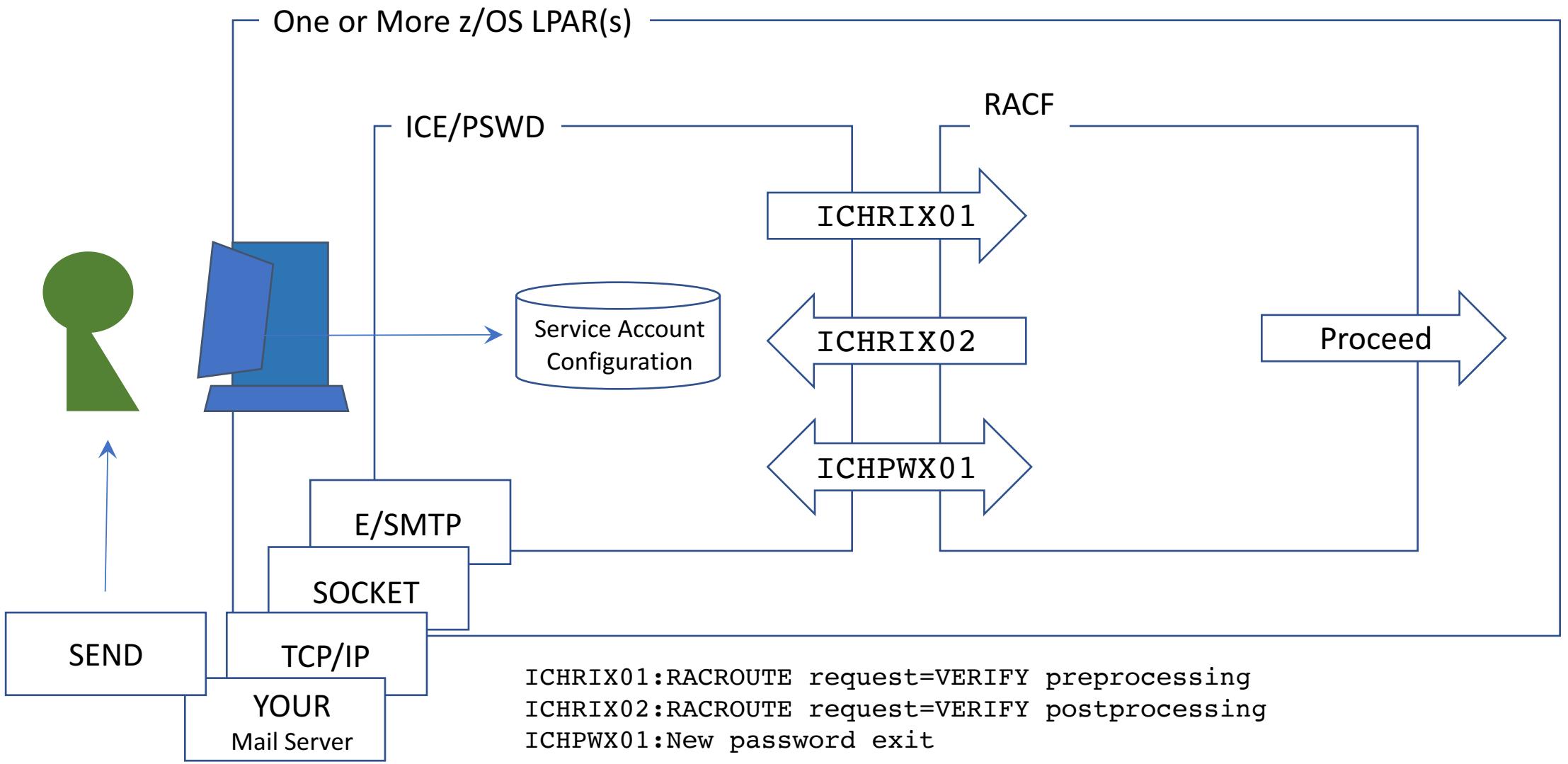
A four ‘Factor’, secure, efficient, 100% software solution for implementing so called MFA on IBM z/OS Systems



Prefix (4/6 characters) and Suffix (4/8 characters)
are changed in a manner that is asynchronous to each other.
Users register/request the Prefix, the System builds/defines the Suffix.
The combination is required for logon during the Validity Window.
When the Window terminates, the process begins anew.

IBM z/OS Security Server RACF - Enrichment

RACF is continuously in control making the final decision to allow/disallow access or reset.



In the unlikely event that ICE becomes inoperable all access control reverts back to native RACF controls