SCADA FEST
ORLANDO | 2026

Proudly Presented by
VTScada
Trihedral
A Delta Group Company

Two Factor Authentication Up Your Security Game

Glenn Wadden, President

User Authentication

- Authentication : Verifying users are who they claim to be.
- Restricts access to resources until the user is verified.
- Must supply authentication **factors** in order to proceed.

2 Factor Authentication (2FA)

- Implemented as a password and another factor, e.g.
  - SMS Text.
  - Voice phone call.
  - Hardware token displaying a code.
  - Push notification to user application or device.
  - Dynamic passcode such as TOTP.
- All the above factors provide varying levels of security and user acceptance.

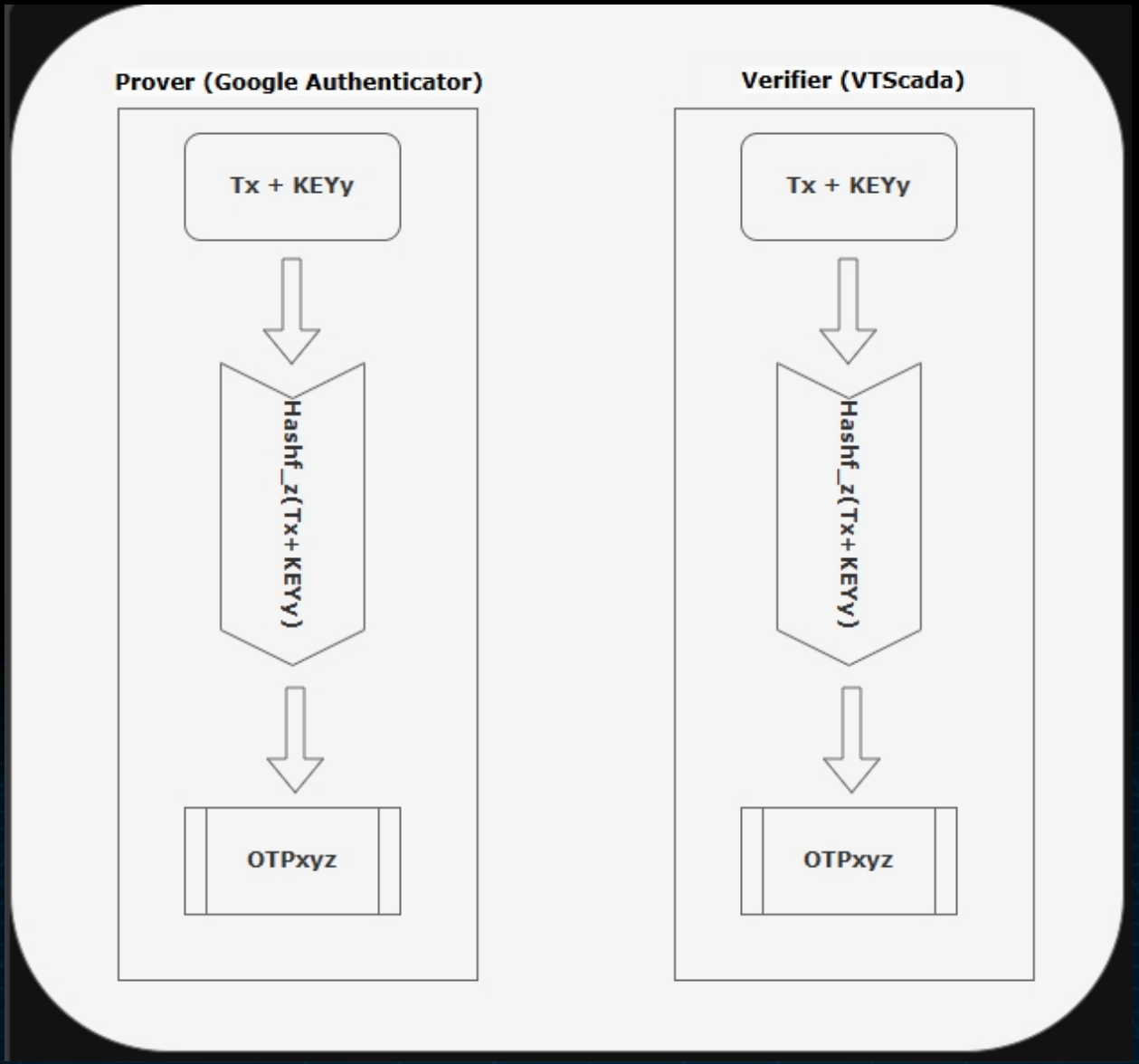
Why TOTP?

- It works when all internet and cell phones are down

TOTP Demo #1

- This demo shows a user starting the sign in process.
  - The user enters their account name and password.
  - The user obtains the OTP code from their authenticator.
  - The user enters the code into the OTP dialog.
  - VTScada verifies the OTP code.
  - The user is signed in.
- This demo also shows a sign in failure with a bad code.

TOTP - Simple algorithm



TOTP essentials

- TOTP uses the current time and a shared secret to generate the OTP codes.
- This requires the clocks on both the VTScada system and the user's authenticator to be closely aligned, ± a few seconds.
- Machine clocks, if not externally controlled, can drift considerably.
- In an Active Directory system, machines usually take their time from the domain controllers (DC's). Obviously, the DC's must get their time from a reliable source.
- For air-gapped systems with no access to an external time source, use of a GPS controlled network time server will be required, approx. $500.

TOTP Authenticators (Provers)

- TOTP authenticators come in many forms, the most common is an application, mobile or desktop.

- Examples include:
  - Microsoft Authenticator
  - Google Authenticator
  - Authy
  - Keeper

Enabling TOTP in VTScada

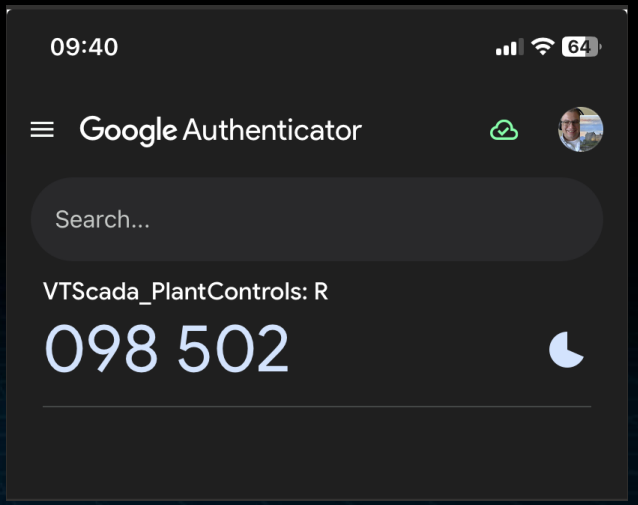
- TOTP is enabled from the “Administrative Settings” dialog.
- Enabling TOTP then requires ALL user accounts to use TOTP.
- User accounts and machines can be exempted from TOTP.
- Disabling TOTP removes ALL TOTP registrations from ALL accounts.

TOTP Registration Demo # 2

- The demo shows an unregistered user attempting to sign in.
- Attendees can also play along in this demo if they have their Authenticator ready!

TOTP Management I

- The Administrative Options dialog allows management of some elements of TOTP operation:
  - Enabling TOTP.
  - Setting the Issuer text.
  - Setting the TOTP window width
  - Exempting workstations from TOTP application.



otpauth://totp/VTSCada_PlantControls:R?secret=KNSWG4TFOQ======&issuer=VTScada&algorithm=SHA1&digits=6&period=30

TOTP Management II

- The Issuer label identifies the TOTP provider. Defaults to “VTScada”, systems with multiple applications should probably have different issuers to allow users to differentiate registrations on their Authenticators.

- The Tolerance Window setting adjusts how “lax” the OTP code verification is. Ideally, leave at the default, but if clocks are not synchronized, it could help.

- Workstation exemptions remove TOTP requirements from specific machines, e.g. access-controlled control rooms.

TOTP Demo #3

- Demonstrates TOTP admin options such as adding and removing workstations from the exempted list.

TOTP Registration Management

- Users can self-register for TOTP if they have the “Modify Account” privilege.
- Users with the “Manager” privilege can initiate registration for other users.
- User account TOTP exemptions can be set by a user with the “Manager” privilege.

TOTP Demo #4

- Demonstrates adding and removing OTP registration on-behalf of another account.

TOTP manual registration

- If the user is unable to scan the QR code with their Authenticator, the secret can be manually added by copying the 32 characters displayed next to the QR code into their Authenticator.

- This is likely to be difficult in the limited time the registration information is displayed.

- If the registration dialog times out before completion, the copied code will NOT be valid, as a new secret will be created for each attempt.

TOTP Exemption Considerations

- Emergency TOTP bypass, e.g. a “break-glass” account.
- Authenticating systems that have no UI, e.g. REST API queries.
- Try to minimize exemptions, too many renders TOTP pointless.

Questions?

Thank you for attending this session!

- Fill out the 2-question feedup survey via the App!
- Especially if you need a Continuing Education Credit or Professional Development Hours certificate.
- Don’t have the app, fill out the paper form included in your conference kit and hand into Natashia.

SAVE THE DATE FOR SCADAFEST 2027!
MARCH 8-12, 2027 | ORLANDO, FL