# Secure Identity and Authentication Management for Shared Wearable AR Displays

- Category: Analysis of Software and Hardware Issues

# Current Situation

- There are more potential users of wearable AR in large enterprises than there are devices available to them
- Some tasks require stereo (binocular) or holographic displays while others can use assisted-reality functionality
- It is too costly and inappropriate to have multiple (or even one) dedicated AR devices for all employees
- In addition, most operators on a shop floor or warehouse do not need to wear AR displays for their full shift but will only need the device to perform dangerous, delicate or urgent tasks.

# Problem this Research Would Address

- When providing multi-user AR displays in the workplace, there is not a keyboard or other input modes which can be used to enter an individual user's credentials
- This hampers secure identification and authentication of the user and delivery of their personalized work instructions to the device they are holding/wearing
- There are no proven technology solutions available or best practices for addressing these obstacles

# Possible Questions the Research Would Answer

- What is currently available for user identification and authentication (sign-in/privacy/security) on multi-user AR display devices?
- Which devices are most often designated as multi-user and why?
- How and when do users get access to AR devices and how are the devices maintained between users?
- What existing technologies can be adapted to the security needs of multi-user displays?
- What are the new technologies that enterprise security departments may need to evaluate and manage as part of their wearable AR security suite in the future?
- What are the requirements and opportunities for new products to address the needs of enterprise security on multi-user wearable AR displays?

# Whose problem would be addressed?

- *Enterprise AR and security managers* would be better prepared
  - To evaluate current vendors/technologies and benefit from the experience of other AREA members (and others in enterprise AR)
  - To implement secure identity and authentication for multi-user AR display in the workplace
- *Providers of enterprise wearable AR displays and enterprise AR software/platform companies* would be able to
  - Through in-house development or by partnering with secure identity and authentication system providers, develop solutions or services that address security needs

# How would this research be conducted?

1. Interview experts who are currently coordinating security policy for wearable AR devices in enterprises and security software vendors
2. Perform desk research and document what other industries (construction, engineering, healthcare) do for other multi-user tools
3. Compile, based on primary and secondary research, examples and develop current best practices/recommendations and methods for testing secure identity and authentication for multi-user AR displays

# Deliverables of this Project

- A report compiling research findings and best practices/recommendations
- An infographic with multiple scenarios and proposed sign-in based on best practices
- Executive summary of findings for public release and a webinar

# Benefits to AREA Members

- An in-depth/best possible understanding the current status of secure identity and authentication systems for multi-user wearable AR displays
- Identification of product and service requirements (and gaps to be addressed)
- Insights for how to best address these challenges now and in the future.