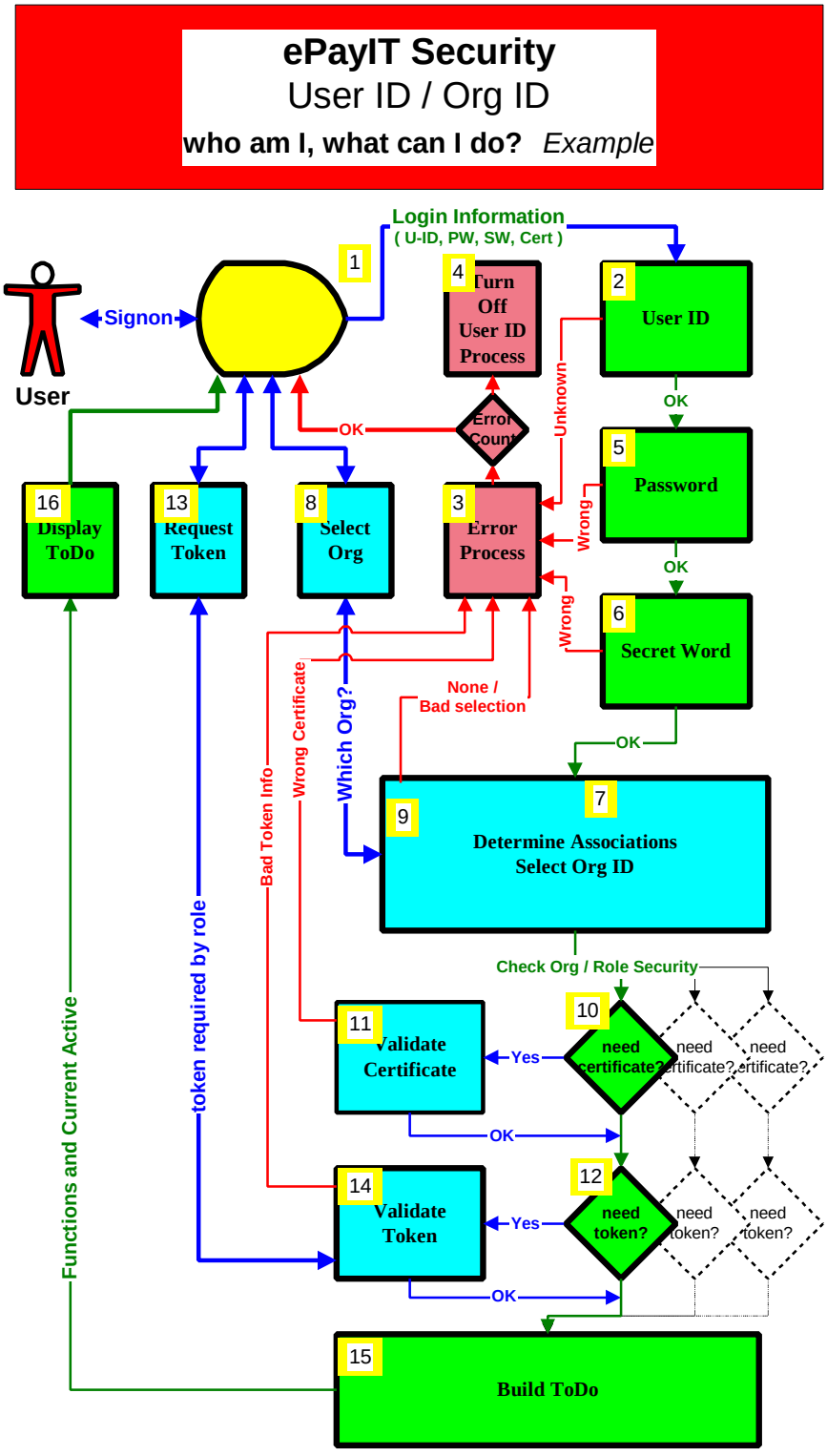
Internet Security

epay it

Table of Contents:

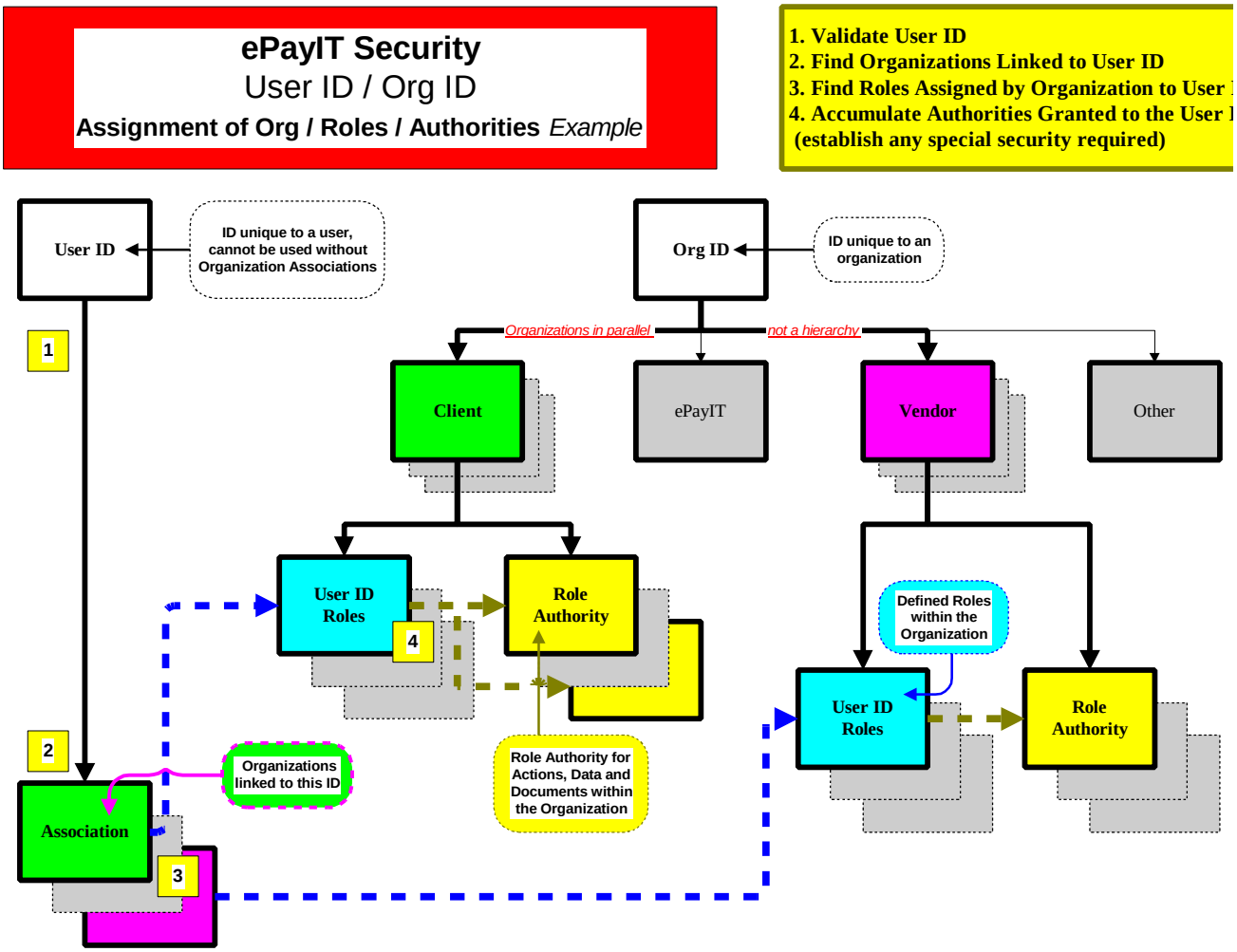
Logon Positive flow:



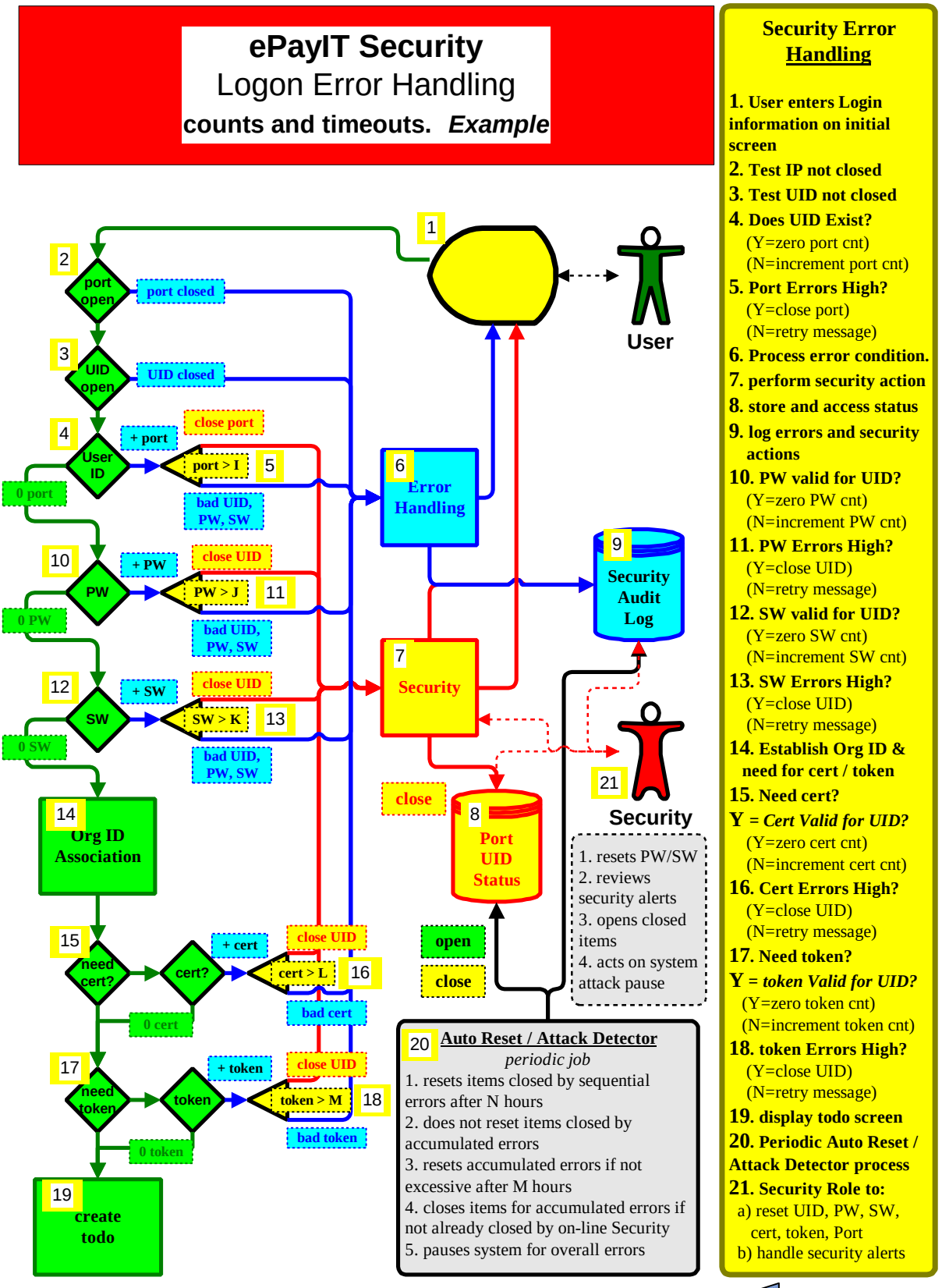
Security Validation Flow

1. User enters Login information on initial screen
2. Validate User ID against active User IDs
3. Update error counts, check error cutoff, display error message
4. Disable User ID, break User ID link to ePayIT
5. Validate Password against User ID Data
6. Validate Secret Word against User ID Data
7. Establish Organization Association of User ID
8. If more than one Org ID association, ask which to use
9. Validate response, establish roles
10. determine need for certificate
11. validate certificate assigned to User-ID
12. determine need for token
13. request token information
14. validate token
15. determine functions for roles, determine active status of todo objects
16. display todo screen

Logon Assignment of Org / Roles / Authorities Example:



Logon Error Flow:



Security Error Handling

1. **User enters Login information on initial screen**
2. **Test IP not closed**
3. **Test UID not closed**
4. **Does UID Exist?**
   (Y=zero port cnt)
   (N=increment port cnt)
5. **Port Errors High?**
   (Y=close port)
   (N=retry message)
6. **Process error condition.**
7. **perform security action**
8. **store and access status**
9. **log errors and security actions**
10. **PW valid for UID?**
    (Y=zero PW cnt)
    (N=increment PW cnt)
11. **PW Errors High?**
    (Y=close UID)
    (N=retry message)
12. **SW valid for UID?**
    (Y=zero SW cnt)
    (N=increment SW cnt)
13. **SW Errors High?**
    (Y=close UID)
    (N=retry message)
14. **Establish Org ID & need for cert / token**
15. **Need cert?**
    Y = ***Cert Valid for UID?***
    (Y=zero cert cnt)
    (N=increment cert cnt)
16. **Cert Errors High?**
    (Y=close UID)
    (N=retry message)
17. **Need token?**
    Y = ***token Valid for UID?***
    (Y=zero token cnt)
    (N=increment token cnt)
18. **token Errors High?**
    (Y=close UID)
    (N=retry message)
19. **display todo screen**
20. **Periodic Auto Reset / Attack Detector process**
21. **Security Role to:**
    a) reset UID, PW, SW, cert, token, Port
    b) handle security alerts

Security Levels:

	0	*1*	*2*	*3*	*4*	***something***
User ID	●	●	●	●	●	You know
Password	●	●	●	●	●	You know
Secret word		●	●	●	●	You know
Certificate			●		●	Browser has
Token				●	●	You have
	View Demo	*View data – some actions allowed*	*Secure User Actions*	*Remote Secure Actions*	*Security Actions*	

END