මාර්ගෝපදේශ අංක: 01/2018

ගෙවීම් පහසුකම් ලබාදෙන ජංගම යෙදුම් මෘදුකාංගයන්ට අදාළ අවම අනුකූලතා ප්‍රමිතීන් සඳහා වූ මාර්ගෝපදේශ

2005 අංක 28 දරන ගෙවීමේ සහ බේරුම් කිරීමේ පද්ධති පනතෙහි, වගන්ති අංක 44 ප්‍රකාරව, බලපත්‍රලාභී වාණිජ බැංකු, බලපත්‍රලාභී විශේෂිත බැංකු, මූල්‍ය සමාගම් හෝ බලපත්‍රලාභී ජංගම දුරකථන ආශ්‍රිත විද්‍යුත් මුදල් පද්ධති ක්‍රියාකරුවන් මෙහෙයවන හෝ ජංගම දුරකථන යෙදුම් මෘදුකාංග ආශ්‍රිත ගෙවීම් සපයන හෝ පහසුකම් සපයන හෝ අදාළ ක්‍රියාවන්හි නිරත වන ඕනෑම ආයතනයක් (මින්මතු ගෙවීම් සේවා සපයන්නන් ලෙස සඳහන්) සඳහා අදාළ වන අවම අනුකූලතා ප්‍රමිතීන් නිර්දේශ කිරීමට මෙකී මාර්ගෝපදේශ නිකුත් කර ඇත.

මෙම මාර්ගෝපදේශ මගින් ජංගම යෙදුම් මෘදුකාංග, වෙබ් සේවා, සේවාදායක පරිගණක දත්ත ගබඩා (Server side databases), ආයචන (Storage) හා පරිගණක සන්නිවේදන ජාල ආදියට පමණක් සීමා නොවී ගෙවීම් සම්බන්ධ ජංගම යෙදුම් මෘදුකාංග ආශ්‍රිත සමස්ථ පද්ධතියම ආවරණය වනු ඇත.

මෙකී මාර්ගෝපදේශ, 2018 ජනවාරි 18 වන දින සිට බලාත්මක වන අතර ගෙවීම් සේවා සපයන්නන් විසින් ක්‍රියාත්මක කරන සියලුම ගෙවීම් ආශ්‍රිත ජංගම යෙදුම් මෘදුකාංග සඳහා ශ්‍රී ලංකා මහ බැංකුවේ අනුමැතිය ලබාගත යුතුය.

2. නිර්වචන/අර්ථ දැක්වීම්

මෙම මාර්ගෝපදේශයෙහි භාවිතා කර ඇති ඕනෑම අවස්ථාවක දී පහත දැක්වෙන පද මෙහි සඳහන් අයුරින් අර්ථ දැක්විය යුතුවේ.

ගිණුම අවහිර කිරීම (Account Lockout)	:	මුරපදය අනුමාන කරමින් යම් ගිණුමකට අනවසරයෙන් පිවිසීමට දරන උත්සාහයේදී නිශ්චිත අසාර්ථක වාර ගණනකට පසු එකී උත්සාහය වැළැක්වීම සඳහා ගිණුම අවහිර කර දැමීමේ ක්‍රමවේදය, ගිණුම අවහිර කිරීම ලෙස හඳුන්වනු ලැබේ.
සත්‍යාපනය (Authentication):	:	පරිශීලකයෙකුගේ අනන්‍යතාව තහවුරු කිරීම හා පරිගණකගත තොරතුරු ලබා ගැනීමට අදාළ පරිශීලකයා සතු සුදුසුකම් පරීක්ෂා කිරීම සත්‍යාපනය ලෙස හඳුන්වනු ලැබේ.
බලය පැවරීම (Authorization)	:	පරිශීලකයාට හෝ සේවාදායකයාට පද්ධතියේ ඇති තොරතුරු හා සම්පත් වෙත ප්‍රවේශ වීමට ඇති වරප්‍රසාද හෝ කුමන මට්ටමේ තොරතුරු වෙත ප්‍රවේශ වීමට ඉඩ සලසනවාද යන්න තීරණය කිරීමේ ආරක්ෂණ ක්‍රමවේදය බලය පැවරීම ලෙස හඳුන්වනු ලැබේ.
උපයෝජ්‍යතාවය (Availability)	:	කාලානුරූපීව හා විශ්වසනීය ලෙස තොරතුරු වෙත පිවිසීමත් ඒවා භාවිතා කිරීමත් සහතික කිරීම උපයෝජ්‍යතාව වේ.
සහතික අධිකාරිය (Certificate Authority)	:	ඩිජිටල් ආයතනයක අන්තර්ජාලයේ ඇති අනන්‍යතාව සත්‍යාපනය කරමින් ඩිජිටල් සහතික නිකුත් කරන විශ්වසනීය ආයතනය, සහතික අධිකාරිය ලෙස හඳුන්වයි.

සහතික ඇමිණීම (Certificate Pinning) : සේවාලාභියා සේවාදායක පරිගණකය සමඟ සබඳතාවක් ගොඩනගන විට සේවාදායක පරිගණකය සිය SSL (Secure Socket Layer) සහතිකය සමගින් ප්‍රතිචාර දක්වයි. මෙකී සහතිකය ජංගම යෙදුම් මෘදුකාංගයට විශ්වාසවන්ත සහතික අධිකාරියක් විසින් නිකුත් කරන ලද එකක් නම් පමණක් සබඳතාවයට අවසර හිමිවේ.

බලපත්‍රලාභී මූල්‍ය අත්පත්කරු (Licensed Financial Acquirer) : බලපත්‍රලාභී මූල්‍ය අත්පත්කරු යන්නෙන් ගෙවීම් මාර්ගයක් ලෙස කාඩ්පත් හිමියන්ගේ ගෙවීම් කාඩ්පත් ප්‍රතිග්‍රහණය කිරීම සහ කාඩ්පත් හිමියන් විසින් මිලදී ගත් භාණ්ඩ හා සේවාවන් වල අගයන් තුන්වන පාර්ශ්වයක් වෙත ප්‍රතිපූරණය කිරීම හා/හෝ කාඩ්පත් හිමියන් විසින් ලබාගත් මුදල් අත්තිකාරම් ප්‍රතිපූරණය කිරීම සඳහා 2013 අංක 01 දරන ගෙවීම් කාඩ්පත් සහ ජංගම දුරකතන ආශ්‍රිත ගෙවීම් පද්ධති සඳහා වන නියෝග යටතේ බලපත්‍ර ලබා ඇති ඕනෑම අයෙකු හෝ ආයතනයක් අදහස් වේ.

සංක්ෂිප්තකරණය/අවම කිරීම (Minification) : මෘදුකාංගයට අදාළ මූලාශ්‍ර කේතයෙහි ක්‍රියාකාරිත්වය නොවෙනස්ව පවත්වා ගනිමින් එහි ඇති අනවශ්‍ය පද ඉවත් කිරීමේ ක්‍රියාවලිය, සංක්ෂිප්තකරණය/අවම කිරීම ලෙස අදහස් වේ.

සංක්ෂිප්ත ගුණනය/අඳුරු කිරීම (Obfuscation) : චේතනාන්විතව තේරුම් ගැනීමට අපහසු කේත නිර්මාණය කිරීම එනම්, මිනිසාට අවබෝධ කර ගැනීමට අපහසු වන මූලාශ්‍ර හෝ යන්ත්‍ර කේතයන් නිර්මාණය කිරීම සංක්ෂිප්ත ගුණනය/අඳුරු කිරීම ලෙස හැඳින්වේ.

වරප්‍රසාද උත්ක්‍රමණය (Privilage Escalation) : මෘදුකාංග යෙදුමක හෝ පරිගණක මෙහෙයුම් පද්ධතියක දෝෂයක්, නිමැවුම් පලුදුවීමක් හෝ ආකෘතියෙහි ප්‍රමාද දෝෂයක් උපයෝගී කර ගනිමින්, පරිශීලකයන් වෙත හෝ යෙදුමක් වෙත සාමාන්‍යයෙන් නිරාවරණය නොකරන දත්ත හා සම්පත් ප්‍රයෝජනයට ගැනීම හෝ ඒ සඳහා උත්සාහ දැරීම වරප්‍රසාද උත්ක්‍රමණය කිරීම වේ.

පරීක්ෂණ අවකාශය (Sand Box) : පරීක්ෂණ අවකාශය යනු භාවිතයේ ඇති ක්‍රමලේඛ වෙන් කර ගැනීමේ ආරක්ෂණ යාන්ත්‍රණයයි. පරීක්ෂා නොකළ හෝ විශ්වාස කළ නොහැකි ක්‍රමලේඛ හෝ කේත ක්‍රියාත්මක කිරීම සඳහා එය නිරතුරුවම භාවිතා වේ.

සංවේදී දත්ත (Sensitive Data) : පාරිභෝගික අක්ත පත්‍ර (Customer Credentials), බැංකු ගිණුම් අංක, ගෙවීම් කාඩ්පත් අංක හෝ ඒ හා සමාන තොරතුරු මෙම සන්දර්භය තුළදී සංවේදී දත්ත ගණයට ඇතුළත් වේ.

කෙටිකාලීන ප්‍රවේශ ටෝකනය (Short-lived Access Token) : සේවාලාභියෙකු (Client) සේවාදායක (Server) පරිගණකය හා සම්බන්ධ වීමට ප්‍රවේශ ටෝකනයක් (Access Token) යොමු කරන අවස්ථාවකදී සේවා දායකය එම ප්‍රවේශ ටෝකනයෙහි ඇති තොරතුරු මත පදනම්ව සේවා ලාභියාගේ අනන්‍යතාවය තහවුරු කර ගනී. මෙකී ප්‍රවේශ ටෝකන කෙටි ආයු කාලයකින් යුතු ඒවා වේ.

පාර්ශ්වකරුවන් (Stakeholders) : ගෙවීම් සේවා සපයන්නන්, මෘදුකාංග විකුණුම්කරුවන්, සේවා සපයන්නන්, ප්‍රතිලාභ ලබන වෙළෙඳුන් හා විගණකවරුන්, මෙම සන්දර්භය තුළදී පාර්ශ්වකරුවන් ලෙස හඳුන්වනු ලැබේ.

URL **සංචාලනය** (Uniform Resource Locattor (URL)) : URL ලිපිනයෙහි පරාමිතීන් වෙනස් කිරීමේ (බොහෝවිට ස්වයංක්‍රීයව) ක්‍රියාවලිය URL සංචාලනය වේ.

3. **ප්‍රතිපත්ති සම්පාදනය** (Policy Formulation)

3.1 සියලුම ගෙවීම් ආශ්‍රිත ජංගම යෙදුම් මෘදුකාංග හැසිරවීම සඳහා ව්‍යාපාරික අරමුණු, ප්‍රමිතීන්, අනුකූලතාවයන්, මාර්ගෝපදේශන, පාලන විධි, වගකීම් හා බැරකම් ආවරණය වන පරිදි ප්‍රතිපත්ති ලේඛනයක් සැකසීම ගෙවීම් සේවා සපයන්නන් විසින් සිදුකළ යුතුය. ඔවුන්ට මෙම ලේඛනය වාර්ෂිකව හා අවැසි අවස්ථාවලදී සංශෝධනය කළ හැකිය.

3.2 සියලුම ගෙවීම් ආශ්‍රිත ජංගම යෙදුම් මෘදුකාංග නිර්මාණය හා සංවර්ධන කටයුතුවලදී මෙම ප්‍රතිපත්ති ලේඛනයෙහි සඳහන් කරුණු රාමුවක් ලෙස යොදා ගත යුතු අතර ඒ පිළිබඳව සියලුම පාර්ශ්වකරුවන් පැහැදිලි ලෙස දැනුවත් කළ යුතුය.

4. **ප්‍රලේඛනය/ලේඛන සම්පාදනය** (Documentation)

4.1 අදාළ සියලුම පාර්ශ්වයන් විසින්, සකසන හා නඩත්තු කරන නිර්මාණ ශිල්ප ක්‍රමවේද (Architecture diagrams), පද්ධති අවශ්‍යතා පිරිවිතර, තාක්ෂණික ලේඛන හා අනෙකුත් පරිශීලක ලේඛන ආදී අවශ්‍ය සියලුම ලේඛන ඉහතින් ඇති 3 වන කොටසෙහි වගන්තිවලට අනුකූලව සකසා ඇති බවට, ගෙවීම් සේවා සපයන්නා විසින් සහතික විය යුතුය.

5. **උපාංග ලියාපදිංචි කිරීම** (Device Registration)

5.1 සිම්පත් අංකය හා මාධ්‍ය ප්‍රවේශ පාලක යොමුව (MAC Address) හෝ අන්තර්ජාතික ජංගම උපකරණ අනන්‍යතා අංකය (IMEI Number) ඇතුළත් උපාංග හඳුනාගැනීමේ තොරතුරු භාවිතා කර, ගෙවීම් සේවා සපයන්නන් විසින් පරිශීලක ගිණුම් සහ ජංගම උපකරණ ලියාපදිංචි කරගත යුතු වේ.

5.2 සෑම ගෙවීම් ආශ්‍රිත ජංගම යෙදුම් මෘදුකාංග පරිශීලක ගිණුමක්ම භාවිතා කිරීමට අවසර ලබාදිය යුත්තේ ගෙවීම් සේවා සපයන්නා සමග ලියාපදිංචි කර ඇති ජංගම උපාංග වලින් පමණි.

5.3 සෑම ගෙවීම් සම්බන්ධිත ජංගම යෙදුම් මෘදුකාංග පරිශීලක ගිණුමක් වෙනුවෙන්ම පිවිසුම් හා මූල්‍ය වටිනාකම මත පදනම් වූ ගනුදෙනු සත්‍යාපන ක්‍රමවේදයක් අනුගමනය කළ යුතුය.

6. **සත්‍යාපනය සහ මුරපද ප්‍රතිපත්ති** (Authentication and Password Policy)

සේවා දායකයේ අන්තයෙන් සත්‍යාපනය කිරීම සඳහා පහත දැක්වෙන අවම පාලන උපක්‍රමයන් හා මුරපද ප්‍රතිපත්ති ක්‍රියාත්මක කළ යුතුවේ.

6.1 සත්‍යාපන ක්‍රියාවලිය සේවාදායක අන්තයෙන් පමණක් සිදු කළ යුතුය.

6.2 ග්‍රාහක ඉල්ලීම් සත්‍යාපන ක්‍රියාවලියේදී පරිශීලකයන්ගේ තොරතුරු (User Credentials) සම්ප්‍රේෂණය නොකළ යුතු අතර ඒ සඳහා කෙටිකාලීන ප්‍රවේශ ටෝකනයක් ක්‍රියාත්මක කළ යුතුවේ.

6.3 සිම්පත් අංකය, උපාංග හඳුන්වනය, මුරපදය/PIN අංකය සහ ගෙවීම් ආශ්‍රිත ජංගම යෙදුමට විශේෂිත වූ මෘදුකාංග හඳුන්වනයක් සමගින් ක්‍රියා කරන බහු සාධක සත්‍යාපන ක්‍රමවේදයක් (Multi Factor Authentication) ක්‍රියාත්මක කළ යුතුය.

6.4 මුරපද වින්‍යාසගත කිරීම (Configuration) සම්බන්ධයෙන් ප්‍රබල ප්‍රතිපත්තියක් ක්‍රියාත්මක කළ යුතුය.

6.5 යම් ගිණුමකට වලංගු නොවන ක්‍රමවේදයක් ඔස්සේ පිවිසීමට උත්සාහ දරන විට, එවැනි උත්සාහ වාර කිහිපයකට පසු ගිණුම අගුලු දැමීමේ ක්‍රියාවලියක් ස්ථාපිත කළ යුතු අතර, එම ගිණුම් නැවත විවෘත කිරීමට අවශ්‍ය වූ විට අදාළ ගෙවීම් සේවා සපයන්නා විසින් ස්ථාපිත සම්මත ආරක්ෂණ ක්‍රමවේදයක් අනුගමනය කළ යුතු වේ.

6.6 ප්‍රවේශ අක්‍රමිකතා සහ සිදුවිය හැකි තත්කාලීන ආක්‍රමණ අනාවරණය කර ගැනීම පිණිස, සත්‍යාපන තැත්කිරීම් පිළිබඳ වාර්තා තබා ගැනීමත් අධීක්ෂණය කිරීමත් කළ යුතුය.

6.7 අභ්‍යන්තර සම්පත්වලට පිවිසුම් නිසි ලෙස සත්‍යාපනය කළ යුතුය.

7. බලය පැවරීම (Authorization)

බලය පැවරීම සම්බන්ධව පහත දැක්වෙන අවම පාලන ක්‍රමවේදයන් ක්‍රියාත්මක කළ යුතුය.

7.1 සෑම අවස්ථාවකදීම, අවම වරප්‍රසාද පිළිබඳ මූලධර්මයන් (Principles of Least Privilege) අනුගමනය කළ යුතුය.

7.2 වරප්‍රසාද උත්ක්‍රමණය හා URL සංචාලනයට අදාළ වන පාලන විධිවිධාන ක්‍රියාත්මක කළ යුතුය.

8. සැසි මෙහෙයවීම (Session Handling)

සැසි මෙහෙයවීමේදී පහත දැක්වෙන අවම පාලනයන් ක්‍රියාත්මක කළ යුතුය.

8.1 සැසි අනන්‍යතා අංකය සසම්භාවීකරණයට ලක්විය යුතුය.

8.2 කිසියම් ගෙවීම් ආශ්‍රිත ජංගම යෙදුමක් වින්‍යාසගත නිශ්චිත කාල පරතරයක් නිද්‍රාශීලීව/අක්‍රීයව පවතින විට එම පරිශීලකයා ස්වයංක්‍රීයව ගිණුමෙන් ඉවත් කිරීම (Automatic User Log Off) කළ යුතුය.

8.3 පරිශීලකයාට පැහැදිලිව පෙනෙන හා පහසුවෙන් භාවිතා කල හැකි ගිණුම් වරන ක්‍රමයක් (Log off method) ක්‍රියාත්මක කළ යුතුය.

8.4 පරිශීලකයා ගිණුමෙන් පිටතට පැමිණෙන විට, අදාළ යෙදුම හා සම්බන්ධ කෙටිකාලීනව හා ස්ථිර ලෙස ගබඩා කරගත් සංවේදී දත්ත ඇත්නම් ඒවා සියල්ල කල් ඉකුත් කිරීම හෝ මකා දැමීම සිදු කළ යුතුවේ.

8.5 ජංගම උපකරණයක් නැතිවී හෝ සොරාගෙන ඇති බවට වාර්තා වූ විට, එම උපකරණයෙන්, අදාළ ගෙවීම් ආශ්‍රිත ජංගම යෙදුම වෙත පිවිසීමට ඇති හැකියාව අක්‍රීය කර දැමිය හැකි මධ්‍යගත ක්‍රමවේදයක් ස්ථාපිත කළ යුතුය. තවද, යම් ගිණුමකට එකවර උපකරණ කිහිපයකින් ඇතුලුවීමට උත්සාහ දරන විට, සේවාදායක අන්තයෙන් ඒ බව හඳුනාගෙන පරිශීලකයා/ගිණුම් හිමියා වෙත ඒ බව සන්නිවේදනය කළහැකි ක්‍රමවේදයක් ස්ථාපනය කළ යුතුවේ.

9. දත්ත ඇතුළු කිරීම සහ ගබඩා කිරීම (Entering and Storing Data)

9.1 බලපත්‍රලාභී මූල්‍ය අත්පත්කරුවෙකුගේ වසමක් (Domain) තුළ හෝ ගෙවීම් ආශ්‍රිත යෙදුම් මෘදුකාංග දත්ත ආරක්ෂණ ප්‍රමිතීන් (PA-DSS) යටතේ හා ගෙවීම් කාඩ්පත් කර්මාන්තය හා සම්බන්ධ ආරක්ෂණ ප්‍රමිතීන් (PCI-DSS) යටතේ සහතිකලත් ජංගම යෙදුම් පද්ධතියක් තුළ දී පමණක් ගෙවීම් කාඩ්පත් ආශ්‍රිත දත්ත ග්‍රහණය කර ගැනීම සිදු කළ යුතුය.

9.2 ගෙවීම් කාඩ්පත් දත්ත හැරුණුවිට සෙසු ගෙවීම් ආශ්‍රිත සංවේදී දත්තයන් ග්‍රහණය කිරීම/ගබඩා කිරීම, ශ්‍රී ලංකා මහ බැංකුව විසින් අනුමත හා නියාමනයන්ට අනුකූල සමස්ථ පද්ධතියක් තුළ පමණක් සිදු කළ යුතුය.

9.3 ගිණුම් අංක සහ අනෙකුත් සංවේදී තොරතුරු ජංගම උපාංගය තුළ ගබඩා නොකළ යුතුය.

9.4 උපාංගයෙහි ඇති සසම්භාවී ප්‍රවේශ මතකය (RAM) තුළ ඇති සංවේදී තොරතුරු සුදුසු පරිදි සුරක්ෂිත කළ යුතුය.

9.5 දත්ත ගබඩා තුළ දත්ත ගබඩා කිරීමට පෙර එම දත්තවල වලංගු භාවය හා සුපිරිසිදු භාවය තහවුරු කළ යුතුය. ගෙවීම් ආශ්‍රිත ජංගම යෙදුම් මෘදුකාංග හා සම්බන්ධ වන දත්ත ගබඩා, සේවාදායක-සේවායෝජක යන දෙඅන්තයෙන්ම (Server side - Client side) නිසි උපක්‍රම යොදා ආරක්ෂාව දැඩි කළ යුතුය.

10. මංගත නොවන ගනුදෙනු (Offline)

10.1 අගය රාශිගත කාඩ්පත් (Stored Value Cards) භාවිතා කළ ගෙවීමක් හෝ ශ්‍රී ලංකා මහ බැංකුව විසින් අවසර දෙන ලද ගනුදෙනු හැරුණු කොට, ගෙවීම් ආශ්‍රිත ජංගම යෙදුම් මෘදුකාංගය, මංගත නොවන ගනුදෙනු (Offline Transactions) සඳහා අවසර දීමක් හෝ පසුකාලීනව සම්ප්‍රේෂණය කිරීමේ අරමුණින් ගනුදෙනුවට අදාළ දත්ත උපාංගය තුළ ගබඩා කිරීමක් නොකළ යුතුය.

11. සංකේතනය (Cryptography)

ගෙවීම් ආශ්‍රිත ජංගම යෙදුම් මෘදුකාංග සංකේතන ඇල්ගෝරිතම සැලසුම් කිරීමේදී හා භාවිතා කිරීමේදී පහත දැක්වෙන ගුණාංග භාවිතා කළ යුතුය.

11.1 ගෙවීම් ආශ්‍රිත ජංගම යෙදුම් මෘදුකාංග සඳහා මූල්‍ය කර්මාන්තය තුළ පිළිගත් සංකේතන ඇල්ගෝරිතම හා සංකේතන විධික්‍රම යොදා ගත යුතුය.

11.2 සංවේදී දත්ත සම්ප්‍රේෂණයේදී (in transit) හා භාවිතයේ නොයොදා පවතින අවස්ථාවන්හිදී ගුප්ත කේතනය (Encrypt) කර තිබිය යුතුය. තවද, ගෙවීම් ආශ්‍රිත ජංගම යෙදුම් මෘදුකාංගවල මුරපද ආරක්ෂණ ක්‍රියාවලියේදී පූරණය (Hashing) කිරීමට අමතරව තවත් කේත උපක්‍රමයක් (Salt) භාවිතා කළ යුතුවේ.

11.3 පූරණයට අදාළ ගණනය කිරීම් මූල්‍ය කර්මාන්ත ප්‍රමිතීන්ට අනුකූල විය යුතුය.

11.4 ගුප්ත කේතනයට අදාළ කේතයන් (Encryption Keys) නිසි ආරක්ෂණ පාලනයන්ට යටත් නොකොට ජංගම උපාංගයේ ගබඩා කර තැබීම නොකළ යුතුය.

12. ප්‍රවාහන ස්තර ආරක්ෂණය

12.1 සියලුම සන්නිවේදනයන් සඳහා ප්‍රවාහන ස්තර ගුප්ත කේතනය (Encrypt) විය යුතුය.

12.2 සහතික ඇමිණීම (Certificate Pinning), යෝග්‍ය විශේෂ ප්‍රතිචාර දැක්වීමේ උපක්‍රම (Exception Handling) සමග නිසිලෙස ක්‍රියාත්මක කිරීම සහ භාවිතා කිරීම සිදු කළ යුතුය.

12.3 සහතික ඇමිණීමේ ක්‍රියාවලිය මගහැර යාමට ඇති අවස්ථා අවම කිරීමට අදාළ පාලනයන් ස්ථාපිත කළ යුතුය.

12.4 SSL සහතිකකරණයේදී දෝෂ පැන නැගුන විට ඒ සඳහා නිසි ක්‍රියා මාර්ග ගන්නා තෙක් ගෙවීම් ආශ්‍රිත ජංගම යෙදුම් මෘදුකාංග ක්‍රියාත්මක වීම නතර කළ යුතු අතර එවැනි දෝෂ සහිත අවස්ථා නොසලකා හැර ඉදිරි පියවර ගැනීම නොකළ යුතු වේ.

12.5 ගෙවීම් ආශ්‍රිත ජංගම යෙදුම් මෘදුකාංග සඳහා විශ්වාසනීය සහතික අධිකාරියක් විසින් නිකුත් කරන ලද වලංගු SSL සහතික භාවිතා කළ යුතුය.

12.6 එක් වරක් පමණක් භාවිතා කරන තාවකාලික මුරපදය (OTP) හැරුණු කොට අනෙකුත් සියලුම සංවේදී දත්තයන් USSD, SMS, MMS හා නිවේදන දැනුම්දීම් ආදී විකල්ප මාධ්‍යයන් භාවිතා කොට සම්ප්‍රේෂණය නොකළ යුතුය.

13. ඉංජිනේරු ප්‍රතිවර්තනය හා නිදොස් කිරීමේ ක්‍රියාවලිය (Reverse Engineering & Debugging)

13.1 ගෙවීම් ආශ්‍රිත ජංගම යෙදුම් මෘදුකාංග ක්‍රියාත්මකව පවතින අවස්ථාවන්හිදී එය නිදොස් කිරීමට හෝ දෝෂහරණ (Debug) සඳහා කිසිදු තෙවන පාර්ශ්වයක් වෙත අවසර ලබා නොදිය යුතුය.

13.2 ගෙවීම් ආශ්‍රිත ජංගම යෙදුම් මෘදුකාංගයෙහි සංක්ෂිප්තකරණය (Minification) සහ සංක්ෂිප්ත ගුණනය (Source Code Obfuscaion) යන තාක්ෂණික ක්‍රමවේදයන් භාවිතා කළ යුතු වේ.

14. අයුතු වෙනස්කිරීම් අනාවරණය (Tampering Detection)

14.1 සේවාදායක අන්තයෙහි (Server Side) අඛණ්ඩතාව තහවුරු කිරීම සඳහාත් සේවාලාභී යෙදුමෙහි යම් අනිසි හැසිරවීමක් ඇත්නම් එය හඳුනාගැනීම සඳහාත් පහත දැක්වෙන පරීක්ෂාවන් ස්ථාපනය කළ යුතුය. ගෙවීම් ආශ්‍රිත ජංගම යෙදුම් මෘදුකාංගය ආරම්භයේදී හෝ සුදුසු අවස්ථාවන්හිදී මෙම පරීක්ෂාවන් ක්‍රියාත්මක කළහැකි අතර එක් පරීක්ෂණයකදී හෝ, කිසියම් අක්‍රියතාවක් හෝ බිඳවැටීමක් ඇති බවට වාර්තා වුවහොත් අදාළ යෙදුම අක්‍රිය කළ යුතුය.

14.1.1 කේත කට්ටල වල පූරණ අගයන් (Hash Values) / ආවේක්ෂණ ඓක්‍යය (Checksum), කේත ආකෘතියේ කොටසක් හෝ සමස්ථ වැඩසටහන.

14.1.2 පද්ධති ගොනුවල ප්‍රමාණය/විශාලත්වය හෝ ගොනු වෙනස් කිරීමේ කාල මුද්‍රාවන් (Time Stamps) තහවුරු කිරීම.

14.1.3 ධාවන කාලය තුළ දී පැකේජයෙහි අනන්‍යතාවය තහවුරු කිරීම.

14.2 මූලාශ්‍ර කේතයන් වෙත පරිශීලකයාට ප්‍රවේශ වීමට අවසර දී ඇති (Rooted/ Jail broken) උපකරණ තුළ ගෙවීම් ආශ්‍රිත ජංගම යෙදුම් මෘදුකාංගය ක්‍රියාත්මක වීමට අවසර ලබා නොදිය යුතුය.

14.3 ගෙවීම් ආශ්‍රිත ජංගම යෙදුම් මෘදුකාංගය ක්‍රියාත්මක වන්නේ නිදොස්කුරු අනාවරණ පසුබිමක (Debugger) හෝ අනුගාමික පසුබිමක (Emulator) ද යන වග අනාවරණය කර ගැනීමට ක්‍රමවේදයක් තිබිය යුතු අතර එවැනි පසුබිමක ජංගම යෙදුම් මෘදුකාංගය ක්‍රියාත්මක වීම ස්වයංක්‍රීයව වැළැක්වීමට ක්‍රමවේදයක් ස්ථාපිත කළ යුතු වේ.

15. ගෙවීම් ආශ්‍රිත ජංගම යෙදුම් මෘදුකාංගය සඳහා අදාළ මෙහෙයුම් පද්ධති අවසරයන්

15.1 ගෙවීම් ආශ්‍රිත ජංගම යෙදුම් මෘදුකාංගය ක්‍රියාත්මක කිරීමට අවශ්‍ය අවම මෙහෙයුම් පද්ධති අවසරයන් පමණක් අත්පත් කර ගැනීමට කටයුතු කළ යුතුය.

16. ආරක්ෂිත කේතනය (Secure Coding)

ගෙවීම් සේවා සපයන්නන් විසින් පහත සඳහන් ක්‍රියාමාර්ග අනුගමනය කළ යුතුය.

16.1 ජංගම යෙදුම් මෘදුකාංග නිර්මාණය කරන පාර්ශ්ව විසින් අදාළ කර්මාන්තය ආශ්‍රිතව පිළිගත් ආරක්ෂිත කේතකරණ භාවිතයන් හා ප්‍රමිතීන් පිළිපැදිය යුතුය.

16.2 ගෙවීම් ආශ්‍රිත ජංගම යෙදුම් මෘදුකාංග සඳහා අවදානම් සහගත/අතහැර දමා ඇති සංරචක, නියමාවලි, පුස්තකාල, තාක්ෂණික පිටපත් ආදිය භාවිතා නොකල යුතුය.

16.3 සංරචක/ නියමාවලි/ පුස්තකාල/ තාක්ෂණික පිටපත් ඇතුළත් කිරීම මත ගෙවීම් ආශ්‍රිත ජංගම යෙදුම් මෘදුකාංගය අවදානම් සහගත තත්ත්වයන් වෙත නිරාවරණය නොවිය යුතුය.

16.4 ගෙවීම් ආශ්‍රිත ජංගම යෙදුම් මෘදුකාංගයෙහි තාක්ෂණික දුබලතා හෝ අවදානම් හඳුනාගත් විගස ඒවාට නිසි පිළියම් යෙදිය යුතුය.

16.5 පරිගණක කේතය තුළ සංවේදී තොරතුරු සෘජු ක්‍රමවේදයක් (Hard Code) ඔස්සේ ඇතුළත් කර නොතිබිය යුතුය.

17. ආදාන හා ප්‍රතිදාන කළමනාකරණය

17.1 සියලුම ආදාන හා ප්‍රතිදාන දත්තවල වලංගුභාවය සහ සුපිරිසිදුභාවය සේවාදායක පරිගණක හා සේවාලාභී පරිගණක දෙඅන්තයෙන්ම තහවුරු කළ යුතුය.

17.2 සංවේදී තොරතුරු ඇතුළත් කිරීමේ දී ස්වයංක්‍රීයව සම්පූර්ණ වීමේ පහසුකම අක්‍රීයව පැවතිය යුතුය.

17.3 සංවේදී දත්ත සම්බන්ධිත කාර්යයන්වල දී පසුරු පුවරුව (Clipbord)/ පිටපත් කර ඇලවීම (Copy-paste) යන පහසුකම් අක්‍රීය කිරීමට අදාළ පාලනයන් ස්ථාපිත කළ යුතුය.

18. දෝෂ සහ විශේෂ අවස්ථාවන් හැසිරවීම

18.1 ජංගම යෙදුම් මෘදුකාංගයෙහි පූර්ණ ක්‍රියාකාරීත්වයම ආරවණය වන පරිදි, නිසි දෝෂ හැසිරවීමේ ක්‍රියාවලියක් ස්ථාපිත කළ යුතුය.

18.2 ජංගම යෙදුම් මෘදුකාංගය පරිශීලනයේ දී දෝෂ සහගත තත්ත්වයන් පිළිබඳ හෝ අනතුරු ඇඟවීම් පිළිබඳ ස්වයංක්‍රීය දැනුම් දීමේ පණිවුඩ තුළ සංවේදී තොරතුරු හෝ ඉඟි ඇතුළත් නොකළ යුතුය.

18.3 ගෙවීම් ආශ්‍රිත ජංගම යෙදුම් මෘදුකාංගයෙහි පැන නගින සියලු දෝෂ සේවා දායක පරිගණක තුළ වාර්තා කර තැබිය යුතුය.

19. සේවාදායක පරිගණක ආශ්‍රිත යටිතල පහසුකම්

19.1 ගෙවීම් ආශ්‍රිත ජංගම යෙදුම් මෘදුකාංගය සමඟ සන්නිවේදනය කරනු ලබන සේවාදායක පරිගණක සහ වෙබ් සේවා නිසි ලෙස සුරක්ෂිත කළ යුතුය.

19.2 සේවාදායක පරිගණක වෙත ප්‍රවේශ පාලනය හා විගණනයන්ට අදාළ වාර්තා සේවාදායක පරිගණක මට්ටමින් පවත්වා ගත යුතුය.

19.3 ගෙවීම් ආශ්‍රිත ජංගම යෙදුම් මෘදුකාංගය මගින් භාවිතා නොකරන දත්ත හුවමාරු දොරටු හා සේවාවන් (Ports and Services) සෑම විටම අක්‍රීය තත්ත්වයේ පැවතිය යුතුය.

20. ලොග් වාර්තා සහ දත්ත කාන්දු වීම/ අන්සතු වීම

සවිස්තරාත්මක ගනුදෙනු පිළිබඳ ලොග් වාර්තා පහත දැක්වෙන පරිදි පවත්වාගෙන යා යුතුය.

20.1 ගෙවීම් ආශ්‍රිත ජංගම යෙදුම් මෘදුකාංගයෙහි ඇතිවන බිඳ වැටීම් පිළිබඳ දත්ත හා වාර්තා, ජංගම උපාංගය තුළ ගබඩා නොකළ යුතුය.

20.2 ගෙවීම් ආශ්‍රිත ජංගම යෙදුම් මෘදුකාංගයෙහි ලොග් වාර්තා තුළ කිසිදු සංවේදී දත්තයක් ඇතුළත් නොවිය යුතුය.

20.3 ලොග් වාර්තාවන් ජංගම යෙදුම් මෘදුකාංගය හා සම්බන්ධ දත්ත සමුදායන්ට අදාළ සේවාදායක පරිගණක වලින් වියුක්තව පවත්වාගෙන යන ලොග් සේවාදායක පරිගණක තුළ ගබඩා කළ යුතු අතර ඒවාට නිසි ප්‍රවේශ පාලන ක්‍රමවේදයන් ස්ථාපිත කළ යුතුය.

20.4 ලොග් වාර්තාවන් වෙනස් කිරීම් හෝ විනාශ කිරීම් වලින් ආරක්ෂා කර ගැනීම සඳහා ආරක්ෂණ ක්‍රමවේදයක් ස්ථාපනය කළ යුතු අතර ඒවා වෙත ප්‍රවේශ වීම අවසරලත් නිලධාරීන්ට පමණක් සීමා කළ යුතුය.

20.5 සේවාදායක පරිගණක සහ සමස්ත පද්ධතියට අදාල ලොග් වාර්තා විගණනය සඳහා ලබා දිය යුතුය.

20.6 ලොග් වාර්තා අවම වශයෙන් වසර 6 ක කාලයක් රඳවාගත යුතු අතර කිසියම් වූ අලාභ හානියකට අදාල තොරතුරු ආරක්ෂා කිරීම සඳහා සුදුසු හා ප්‍රමාණවත් පියවර ගත යුතුය.

21. ගෙවීම් ආශ්‍රිත ජංගම යෙදුම් මෘදුකාංග කේතයන්හි කතෘ තහවුරු කර ගැනීමේ ක්‍රමවේදය

21.1 මෘදුකාංගයෙහි කතෘ සහතික කිරීම සඳහාත්, එහි කේතය වෙනත් පාර්ශ්වයක් විසින් පසුව වෙනස්කර හෝ විකෘති කර නොමැති බවට සහතික කිරීම සඳහාත්, ගෙවීම් ආශ්‍රිත ජංගම යෙදුම් මෘදුකාංග වෙත ඩිජිටල් කේත අත්සන් ක්‍රමවේදයක් (Code Signing) භාවිතා කරන බව ගෙවීම් සේවා සපයන්නා විසින් තහවුරු කළ යුතු වේ.

21.2 ගෙවීම් ආශ්‍රිත ජංගම යෙදුම් මෘදුකාංගයෙහි ඩිජිටල් කේත අත්සන සඳහා භාවිතා කරන ආවේනික යතුරු කේතය (Private Key) උත්පාදනය කිරීම, සුරක්ෂිතව ගබඩා කිරීම හා උපස්ථායනය යන කරුණුවලට අදාළ ක්‍රියාවන් ගෙවීම් සේවා සපයන්නා විසින් සිදු කළ යුතුය.

21.3 ඩිජිටල් කේත අත්සන් ක්‍රමවේදය සමඟ ප්‍රබල ආවේනික යතුරු කේතයක් (Strong Private Key) සකස් කළ යුතුය.

22. තෙවන පාර්ශ්වයක් සතු යෙදුම් මෘදුකාංග ගබඩා භාවිතා කිරීම හා ව්‍යාපාරික වෙබ් අඩවි වෙත සත්කාරකත්වය ලබා දීම

22.1 Google Play Store, Apple Store හා Windows Store ආදී අනුමත යෙදුම් ගබඩාවල පමණක් ගෙවීම් ආශ්‍රිත ජංගම යෙදුම් මෘදුකාංගය ගබඩා කළ යුතු අතර ගෙවීම් සේවා සපයන්නාගේ වෙබ් අඩවියෙහි හෝ විකුණුම්කරුගේ වෙබ් අඩවියෙහි හෝ වෙනත් තෙවන පාර්ශ්වයක් සතු වෙබ් අඩවියකින් ලබා ගැනීමට හැකිවන පරිදි ස්ථාපිත කර නොතිබිය යුතුය.

22.2 ගෙවීම් ආශ්‍රිත ජංගම යෙදුම තෙවන පාර්ශ්වයක් සතු යෙදුම් ගබඩාවන් තුළ ස්ථාපනය කර නොමැති බව සියලුම පරිශීලකයින් දැනුවත් කර ඇති බවට අදාළ යෙදුම් මෘදුකාංගයේ හිමිකරුවන් විසින් තහවුරු කළ යුතුය.

23. කාර්ය අඛණ්ඩතාව හා සංශෝධන කළමනාකරණය

23.1 මෘදුකාංග සංවර්ධනය කිරීමේ ජීවන චක්‍රය (SDLC) ඇතුලු පද්ධතියේ විස්තර, සංශෝධන කළමනාකරණයට අදාළ තොරතුරු සමඟ නිසි ආකාරව ලේඛන ගත කළ යුතුය.

23.2 තෙවන පාර්ශ්වීය මෘදුකාංගයක් භාවිතා කරන්නේ නම්, ගෙවීම් ආශ්‍රිත ජංගම යෙදුම් මෘදුකාංග හිමිකරු සතුව ජංගම යෙදුම් මෘදුකාංගයට අදාළ ප්‍රභව කේතයට හා එහි සියලු සංශෝධිත අනුවාදයන් සඳහා යෝග්‍ය එස්ක්‍රෝ විධිවිධානයක් (Escrow Arrangement) ඇති බව ගෙවීම් සේවා සපයන්නා විසින් තහවුරු කළ යුතු වේ.

23.3 ගෙවීම් සේවා සපයන්නා විසින් යෝග්‍ය ආපදා ප්‍රතිසාධන (Disaster Recovery) සහ අතිරික්තතා (Redundancy) පද්ධතීන් පවත්වාගෙන යා යුතුය.

23.4 ගෙවීම් ආශ්‍රිත ජංගම යෙදුම් මෘදුකාංග අනුවාද පිටපත් පාලන (Version Controlling) ක්‍රමවේදයක් පවත්වා ගැනීම හා ලේඛනගත කිරීම සිදු කළ යුතුය.

23.5 ගෙවීම් ආශ්‍රිත ජංගම යෙදුම් මෘදුකාංගයට අදාළ සියලුම සංශෝධන සඳහා සුදුසු සංශෝධන කළමනාකරණ කාර්ය පටිපාටියක්/ සංශෝධන සඳහා ඉල්ලීම් ක්‍රමවේදයක් අනුගමනය කළ යුතුය.

24. විගණනය

24.1 වෙබ් සේවා, සේවා දායක පරිගණක, දත්ත ගබඩා සහ සන්නිවේදන ජාල ඇතුලු ගෙවීම් ආශ්‍රිත ජංගම යෙදුම් මෘදුකාංගයට අදාළ සමස්ත පද්ධතිය සඳහා තොරතුරු පද්ධති විගණනයක් සහ තොරතුරු ආරක්ෂණය සම්බන්ධව විගණනයක් සිදු කළ යුතු අතර මෙම විගණනය තොරතුරු පද්ධති විගණනය සම්බන්ධ ප්‍රාමාණික හැකියාවක් ඇති ස්වාධීන, පිළිගත් තෙවන පාර්ශ්වීය විගණකවරයෙකු මගින් සිදු කළ යුතු වේ.

24.2 ස්ථිතික හා ගතික ආරක්ෂණ විශ්ලේෂණයක්, මූලාශ්‍ර කේත සමාලෝචනයක්, නිෂ්පාදන හා පරීක්ෂණ පරිසරය පිළිබඳ විවරණයක්, අවදානම් තක්සේරුකරණයක් හා අනවසර ඇතුලු වීම් මගින් පද්ධතියේ ස්ථායීතාවයට හානිවිය හැකි අවස්ථා පිළිබඳ විමර්ශනයක් යන කරුණු සමග වෙනත් අවශ්‍ය අංග ඇතුළත්වන පරිදි විගණන විෂය පථය ස්ථාපනය කළ යුතුය.

24.3 ගෙවීම් ආශ්‍රිත ජංගම යෙදුම් මෘදුකාංගයට අදාළව මුදා හරින එක් එක් නිකුතුන් (Software Releases), මෘදුකාංගය සජීවී ලෙස ක්‍රියාත්මක කිරීමට පෙර, මෙම මාර්ගෝපදේශ සහ තොරතුරු ආරක්ෂණ විගණන අවශ්‍යතාවලට අනුකූල විය යුතු අතර අදාළ සියලුම යාවත්කාලීන කිරීම් හා දෝෂ ආවරණ කටයුතුවල දී සිදුවන වෙනස්කම් ද එහි ඇතුළත් විය යුතුය.

24.4 සියලුම සම්පාදිත විගණන වාර්තාවන් තුළ විගණන කණ්ඩායමෙහි සියලුම සාමාජිකයන්ගේ වෘත්තීමය අත්දැකීම්, ශාස්ත්‍රීය හා වෘත්තීය සුදුසුකම් ඇතුලු විස්තර ඇතුළත් විය යුතුය.

සී.ජේ.පී. සිරිවර්ධන
නියෝජ්‍ය අධිපති