ඩිජිටල් අත්සන සහ ඩිජිටල් සහතික සම්බන්ධයෙන් <u>නිතර අසනු ලබන ප්‍රශ්න</u>

රාජ්‍ය ආයතනයන්හි ඩිජිටල් පරිවර්තනයක් සඳහා පහසුකම් සැලසීම සඳහාවූ වැඩපිලිවලේ ඩිජිටල් අත්සන් සහ ඩිජිටල් සහතික භාවිතයට අදාළ පහත මාර්ගෝපදේශ ශ්‍රී ලංකා තොරතුරු හා සන්නිවේදන තාක්ෂණ නියෝජිතායතනය විසින් නිකුත්කර ඇත.

මෙය 'සාමාන්‍ය' (general) සහ 'තාක්ෂණික' (technical) ලෙස වර්ගීකරණය කර ඇත. පොදුවේ 'සාමාන්‍ය' කරුණු අවශ්‍ය වන්නේ ඩිජිටල් අත්සන ක්‍රියාත්මක කිරීමට සැලසුම් කරන රජයේ නිලධාරීන් සඳහා වන අතර තාක්ෂණික වශයෙන් කටයුතු කරන නිලධාරීන් සඳහා වඩාත් විස්තරාත්මක කරුණු දැනගැනීම වැදගත්වේ.

1) සාමාන්‍ය කරුණු (General Information)

1.1 ශ්‍රී ලංකාවේ විද්‍යුත් සන්නිවේදනය සහ විද්‍යුත්ගනුදෙනු සඳහා ඇති නීතිමය පිළිගැනීම කුමක්ද?

සියලුම ඉලෙක්ට්‍රොනික සන්නිවේදන හා ගනුදෙනු සම්බන්ද නීතිමය ප්‍රතිපාදන සපයන්නේ 2006 අංක 19 දරන විද්‍යුත්ගනුදෙනු පනත සහ 2017 අංක 25. විද්‍යුත්ගනුදෙනු (සංශෝධන) පනත මගිනි.

ශ්‍රී ලංකාවේ සිදුකෙරෙන සියලුම ඉලෙක්ට්‍රොනික සන්නිවේදනය සහ ගනුදෙනු අදුනාගැනීම, ඒ සඳහා පහසුකම් සැපයීම එමගින් ආවරණයකරයි. එමෙන්ම සියලුම දත්ත පණිවිඩ නිර්මාණය කිරීම සහ හුවමාරු කිරීම, විද්‍යුත් ලේඛන, ඉලෙක්ට්‍රොනික වාර්තා, සැපයීම මෙමගින් ආවරණය කරයි. එක්සත් ජාතීන්ගේ විධිවිධාන අනුව ක්‍රියාත්මක කෙරෙන ජාත්‍යන්තර ගනුදෙනු සඳහාවූ ඉලෙක්ට්‍රොනික සන්නිවේදන භාවිතය පිළිබඳ සම්මුතියට අනුව, සහතික කිරීමේ අධිකාරියක් පත්කිරීම සහ බලපත්‍ර ලබාදීම සහ බලය පැවරීම සඳහා, සහතික කිරීමේ සේවා සපයන්න න්සඳහාද මෙම පනත බලාත්මකාවේ.

1.2 ඉලෙක්ට්‍රොනික වාර්තාවක් යනු කුමක්ද?

ඉලෙක්ට්‍රොනික් වාර්තාවක් යනු ඉලෙක්ට්‍රොනිකව නිර්මාණය කර තැන්පත්කර ඇති ඉලෙක්ට්‍රොනිකව සන්නිවේදනය කළහැකි වාර්තා, ලිඛිත ලේඛනයක් හෝ වෙනත් නිර්මාණයකි.

1.3 ඉලෙක්ට්‍රොනික වාර්තා ශ්‍රී ලංකාවේ නීතියෙන් පිළිගනු ලබන්නේද ?

ඔව්, නීතියෙන් පිළිගනු ලැබේ. 2006 ඉලෙක්ට්‍රොනික ගනුදෙනු පනතේ අංක 19 හි 3 වැනි වගන්තිය, 2017 අංක 25 පනත මගින්කල සංශෝධිතයට අනුව එය විද්‍යුත් ස්වරූපයෙන් පවතින බව පිළිගැනීම, බලපෑම, වලංගුභාවය හෝ බලාත්මක කිරීමේ හැකියාව හදුනා ගැනේ. හදුනා නොගන්නා දත්ත පණිවිඩ, විද්‍යුත් ලේඛනය, ඉලෙක්ට්‍රොනික වාර්තා හෝ වෙනත් සන්නිවේදන නිත්‍යානුකූල නොවන ඒවා ලෙස ප්‍රතික්ෂේප කිරීමද මෙමගින් සිදුවේ.

1.4 ඩිජිටල් අත්සනක් යනු කුමක්ද?

ඩිජිටල් අත්සන් (සම්මත ඉලෙක්ට්‍රොනික අත්සන්) යනු සාම්ප්‍රධායිකව කඩදාසි මත සිදුකරන අත්සන ඉලෙක්ට්‍රොනික සලකුණක් බවට පත් කිරීමයි. මෙම ඉලෙක්ට්‍රොනික සලකුණ හෝ සංකේතාත්මක පණිවිඩය, අත්සන් කරන්නාට අනන්‍යවන අතර එය අනින් සිදුකරන අත්සනක්මෙන් පිළිගනිමින් ඩිජිටල් අත්සන යවන්නාගේ සත්‍යතාව සහතික කරයි.

ලේඛනය; ලේඛනයක මෙම අත්සන් තැබීමෙන් පසුව ම වෙනස්කමක් සිදු කිරීම එය අවලංගුවීමට හේතුවේ.

අත්සන; එමගින් අත්සන ව්‍යාජ භාවිතාකිරීම හා නොරතුරු විකෘති කිරීමෙන් ආරක්ෂා කරමින් ඩිජිටල් අත්සන් කරන්නාගේ අත්සනේ සත්‍යතාව, වගවීම, දත්ත අඛණ්ඩතාව , ලේඛන සහ ගනුදෙනු ප්‍රතික්ෂේප නොවන ලෙස පවත්වාගනයනු ඇත.

1.5 ඩිජිටල් අත්සන් වල වාසි මොනවාද?

ඩිජිටල් අත්සන් බොහෝ ප්‍රතිලාභ ගෙනදෙන අතර ඉන් ප්‍රධාන කරුණු කීපයක් පහත දැක්වේ .

- **වියදම අවමකිරීම**: කඩදාසි රහිත ලියකියවිලි හඳුන්වාදීම දීම මගින් ඒවා කළමනා කරණය කර බෙදාගැනීම කළහැකි බැවින් භෞතික සම්පත් සහ කාලය, පිරිස් සහ කාර්යාල අවකාශය සඳහාවන වැය අවම කරයි.
- **ධනාත්මක පාරිසරික බලපෑම:** කඩදාසි භාවිතය අඩු කිරීමනිසා ලිපිගොනු එහාමෙහා ගෙනයාම වැනි භෞතික ක්‍රියාකාරකම් අඩු කරයි. කඩදාසි මගින් ජනනය වන අපද්‍රව්‍ය සහ අහිතකර පාරිසරික බලපෑම අවම කරයි.
- **පහසුව:** ඩිජිටල් අත්සන් කරන ලද ලේඛන, භෞතික ලේඛන හැසිරවීමට වඩා පහසුය.
- **සොයාගැනීමේ හැකියාව**: සෑම දෙයක්ම ඩිජිටල් ලෙස පවිගත කර ගබඩා කළ පසු, අභ්‍යන්තර වාර්තා තබා ගැනීම පහසු කරවන අතර විගණන කටයුතු සිදුකිරීමද පහසුවනු ඇත. අනින් අත්සන් කරන්නෙකුට හෝ වාර්තා තබන්නෙකුට ලේඛනයක් වැරදීම හෝ අස්ථානගත වීම සිදුවීමට ඇති අවස්ථා අඩුවේ.
- **දින මුද්‍රා තැබීම**: කොටස් වෙළඳාම්, ටෙන්ඩර් ඉදිරිපත් කිරීම් සහ නීතිමය කටයුතු සඳහා කාලය තීරණාත්මක වන විට ඩිජිටල් අත්සනක කාලයකළමනා කරණය සඳහා යෝජනවත් වේ.
- **ගෝලීය පිළිගැනීම සහ නෛතික අනුකූලතාව**: පොදු ප්‍රධාන යටිතල පහසුකම් (PKI) සැපයීමේදී ප්‍රමිතීන්ට අනුව සේවා සපයන්නන් විසින් ඉදිරිපත්කරන සිල් තබන ලද ඩිජිටල් අත්සන යෙදු ලේඛන නීතිමය ලේඛන ලෙස ජාත්‍යන්තර සම්මතය ට අනුව පිළිගනිම වැඩිවෙමින් තිබේ .
- **කාලය ඉතිරිකිරීම්:** ඩිජිටල් අත්සන් මගින් භෞතිකව ගතවන කාලය ඉතිරිකරන අතර ක්‍රියාවලීය සරල කරයි. ලේඛන අත්සන් කිරීම, ගබඩා කිරීම සහ හුවමාරු කිරීම, ව්‍යාපාරකටයුතුවලදී ඉක්මනින් ප්‍රවේශ වීමට ඇති හැකියාව වේගවත්වේ.

1.6 ඩිජිටල් අත්සන් කරන ලද ලේඛන ශ්‍රී ලංකා අධිකරණය විසින් පිළිගනු ලබන්නේද?

ඔව්, ඉලෙක්ට්‍රොනික ගනුදෙනු පනතට අනුව ඩිජිටල් අත්සන් නීත්‍යානුකූලව පිළිගැනේ.2006 අංක 19. පනතේ 7 වැනි වගන්තියේ 2017 අංක 25 දරන සංශෝදිත පාර්ලිමේන්තු පනත මගින් ඩිජිටල් අත්සන තැබූ ඕනෑම ලියවිල්ලක් පිලිගන්නාබව තහවුරුකොට ඇත. ඒ අනුව කිසියම් පුද්ගලයෙකුගේ අත්සන හෝ සහතික කරනලද ඩිජිටල් අත්සන නීත්‍යානුකූල තහවුරුකිරීමක් සේ සලකා තෘප්තිමත් වූ බව සලකනු ලැබේ.

1.7 ඩිජිටල් අත්සන යන්නෙන් අදහස් කරන්නේ භෞතික අත්සනක රූපය යම් ලේඛනයක විද්‍යුත්ලෙස ඇලවීමයි ද ?

නැත. ඩිජිටල් අත්සන ලෙස ලෙස අප හදුන්වන්නේ එය නොවේ. භෞතික අත්සනක රූපය විද්‍යුත් ලෙස ඇලවීමෙන් ලේඛනයක් වලංගු නොවේ. එමගින් සිදුවන්නේ එම ලේඛනය දැක්කා හෝ අනුමත කර ඇතිබවයි. එය තුන්වන පාර්ශවයකට වුව සිදුකර අත්සන හිමිකරුගේ දැනුවත්භාවයකින් තොරව කල හැකිය. එමනිසා එවැනි ලේඛන නීත්‍යානුකූලව පිළිගනු නොලැබේ.

1.8 ඩිජිටල් ලෙස අත්සන් කරන ලද ලේඛනයක මුද්‍රණය (දෘඪ පිටපත)පිටපතක වලංගු භාවයක් තිබේද?

නැත, ඩිජිටල් අත්සනක් ඇලවිය හැක්කේ මෘදු පිටපතකට පමණි. ඩිජිටල් අත්සන තහවුරු කිරීම සඳහා මුල් මෘදු පිටපත තුළ එය තිබිය යුතුය. මුද්‍රණය කරන ලද (දෘඪ පිටපත) වලංගු භාවයක් නොමැත. එම හේතුව නිසාම, ඩිජිටල් ලෙස අත්සන් කරන ලද දෘඪ පිටපත් ගබඩා කිරීමේ තේරුමක් නැත. ඒවා වලංගු කිරීම සඳහා ඉලෙක්ට්‍රොනික ආකෘතියෙන් ගබඩා කළ යුතුය.

1.9 ස්කෑන් කරන ලද ලේඛනයක්/රූපයක් ඩිජිටල් ලෙස අත්සන් කළ හැකිද?

ඔව්. මෘදු soft ස්වරූපයෙන් ඕනෑම ලේඛනයක් ඩිජිටල් ලෙස අත්සන් කළ හැකියි. ලේඛනය ඉලෙක්ට්‍රොනිකව පිටපත්කර හෝ ස්කෑන් කර අත්සන තැබීම ගැටළුවක් නොවේ.

1.10 අත්සන් කරන්නා හෝ වෙනත් අයෙකු ඩිජිටල් ලෙස අත්සන් කරන ලද ලේඛනයේ අන්තර්ගතය වෙනස් කළහොත් කුමක් සිදුවේද?

එසේ අන්තර්ගතය වෙනස්කළහොත් අත්සන් කරන ලද එම ලේඛනය වෙනස් කරන ලද මොහොතේම එම මුල් අත්සන අවලංගුවේ. එය වෙනස්කරනලද ලේඛනයක් ලෙස හදුනාගනු ඇත.

ICTA
ideas actioned
Information and Communication Technology Agency

1.11 එසේ කිරීමෙන් පසු ලේඛනයක් ඩිජිටල් ලෙස අත්සන් කිරීම ප්‍රතික්ෂේප කළ හැකිද?

නැහැ. ඩිජිටල් අත්සන් යෝජනාවලිය පදනම්ව ඇත්තේ දෘශ්‍යමාන නොවන රහස්‍ය ලේඛනමය පදනමකිනි. ඒ අනුව එය නැවත කල නොහැකි ප්‍රතික්ෂේප කිරීමක්ද සිදුවිය හැකියි. එනම් අත්සන් කරන්නාට එය සාර්ථකව කළ නොහැකි අතර ඔහුගේ පුද්ගලික ප්‍රවේශය ද රහසක්ව තබනු ඇත.

1.12 ඩිජිටල් සහතිකයක් යනු කුමක්ද?

සියලුම තාක්ෂණික තොරතුරු පසෙකින් තිබිය දී, සරලව ගතහොත් ඩිජිටල් සහතිකයක් යනු, ඩිජිටල් ලෙස අත්සන් කරනලද වාර්තාවක් හෝ විද්‍යුත් අනන්‍යතාවකි. එය හිමිකරුගේ අනන්‍යතාව තහවුරුකළ ඉලෙක්ට්‍රොනිකව සහතිකකරණ ලද්දකි . එය හිමිකරුගේ අනන්‍යතාව සහතික කරනලද ලේඛනයක් හෝ විද්‍යුත් අක්තපත්‍රයක් ලෙස භාවිතා කල හැකියි (පොදු සහ පුද්ගලික - තාක්ෂණික විස්තරය බලන්න විස්තරාත්මක පැහැදිලි කිරීමක් සඳහා), එය තොරතුරු සංකේතනය කිරීමට සහ ඩිජිටල් ලෙස අත්සන් කිරීමට භාවිතා කළ හැකිය. සහතික නොමැතිව, කෙනෙකුට පුද්ගලික මුරපදය සමඟ සංකේතනය කළ දත්ත යැවිය හැකිය. දත්ත විවරකර ගැනීමට පොදු මුරපදය භාවිතා කරනු ඇත, නමුත් ඕනෑම කෙනෙකුට එය කලහැකි නිසා ඒ පිළිබඳ සහතිකයක් දිය නොහැක. වලංගු මුරපදයක් භාවිතාකිරෙමෙන් පමණක් ග්‍රාහකයාට දැනගත හැකිය. සාරාංශයක් ලෙස, සහතිකකිරමේ අධිකාරියක් හෝ අධිකාරි ආයතනයකට ප්‍රවේශ අනන්‍යතාවය තහවුරු කර ගැනීමට විද්‍යුත් තැපෑලෙහි නමට හෝ වෙනත් එවැනි තොරතුරුවලට ගැලපීම සඳහාවූ තෙවන පාර්ශවිය සත්‍යාපන ක්‍රියාවලියකින් විශ්වාශය තහවුරු කර ගත හැකිය.

1.13 කෙනෙකුට ඩිජිටල්ලෙස අත්සන් කරන ලද ලේඛන (ඩිජිටල් සහතික) අවශ්‍ය වන්නේ ඇයි?

ඩිජිටල් ලෙස අත්සන් කරන ලද ලේඛනයක් යවන්නාගේ අනන්‍යතාවය ඩිජිටල් ලෙස සත්‍යාපනය කරයි. එය ද ඉහළ මට්ටමේ ආරක්ෂාවක් සමඟින් ඔන්ලින් සහතික කිරීම මගින් සබැඳි ගනුදෙනු සඳහා පහසුකම් සපයයි. එවැනි හුවමාරු වන තොරතුරු වල පෞද්ගලිකත්වය ආරක්ෂාවන අපේක්ෂිත ලබන්නාට පමණක් කියවිය හැකි ආකාරයෙන් කෙනෙකුට ඩිජිටල් අත්සන් භාවිතා කළ හැකිය. එය හුවමාරුවේදී වෙනස් කර නොමැති බව ලබන්නාට සහතික කිරීමත් හුවමාරුව සහ පණිවිඩය යවන්නා ලෙස කෙනෙකුගේ අනන්‍යතාවය තහවුරු කිරීමත් මෙමගින් සිදුවේ.

විද්‍යුත් වාණිජ්‍යය භාවිතා කරන්නන් සඳහාද සත්‍යාපනය තීරණාත්මක ගැටලුවකි. ලැබුණු විද්‍යුත් ගනුදෙනුවක සත්‍යතාව සහ අඛණ්ඩතාව පිළිබඳ විශ්වාසය මෙන්ම අනෙකුත් බැංකු හා ගන්දෙනුකිරීමේ හැකියාව මෙම බැංකු සතුව තිබිය යුතුය.

ඩිජිටල් අත්සන භාවිතයෙන් මෙය සාක්ෂාත් කරගත හැකිය. ඩිජිටල් අත්සන ඉලක්ක කර ඇත්තේ භෞතික අත්සනින ලබාගත නොහැකිවන්නාවූ, වඩා ඉහළ මට්ටමේ විශ්වාසයක් සාක්ෂාත් කර ගැනීමයි. ඩිජිටල් අත්සන් කිරීමේ විද්‍යුත් ගනුදෙනුව මගින් ගනුදෙනුව අත්සන් කිරීමෙන් පසු වෙනස්කම් සිදු කර ඇත්නම් එය කුමන පාර්ශවයකින් කරන ලද්දක් දැයි නිසැකවම දැනගත හැකියි.

1.14 ඩිජිටල් සහතික ක්‍රියාකාරිත්වය තුළ සහතික කිරීමේ අධිකාරියක් (Certificate Authority "CA") යනු කුමක්ද?

සහතික කිරීමේ අධිකාරිය (Certification Authority "CA") යනු ඩිජිටල් සහතික නිකුත් කරන ආයතනයයි. යම් සංවිධානයක පුද්ගලන්ගේ හෝ සංවිධානයේ සත්‍යතාව ඔප්පු කිරීමට අත්සන් සහතික නිකුත්කිරීමට කරනු ලබන ඉල්ලීම් මෙමගින් සපුරාලයි. යම් ආයතනක ඩොමේන් පාලන සත්‍යාපනය කළමනාකරණය කිරීමේ වගකීම් සහතික කිරීමේ බලය අධිකාරිය සතුවේ. යම් ආයතනයක ඉල්ලීම මත පොදු ප්‍රවේශයන් සමග ඇති සහතිකකිම් පරිශීලකයාට අයත්බව තහවුරුකිරීම් මෙමගින් සිදුවේ. ඒ අනුව පොදු ප්‍රවේශ පහසුකම් ක්‍රියාවලියේ PKI මෙන්ම අන්තර්ජාල භාවිතයේ ආරක්ෂාව පිළිබඳ වැදගත් කාර්යභාරයක් මෙමගින් සිදුවේ.

1.15 ශ්‍රී ලංකාවේ ඩිජිටල් අත්සන සහතික කිරීමේ අධිකාරී බලය ඇත්තේ කාටද ?

ශ්‍රී ලංකා මහා බැංකුව විසින් මූල්‍ය අංශය සඳහා ඩිජිටල් අත්සන් සහතික කිරීමේ අවශ්‍යතාවය හඳුනාගනිමින් 2006 වසරේ අංක 19 දරන ඉලෙක්ට්‍රොනික ගනුදෙනු පනතට අනුව සේවා සපයන්නා ලෙස LankaClear (Pvt.) Ltd (LCPL) ආයතනයේ LankaSign යන වෙළඳ නාමය යටතේ ශ්‍රී ලංකාවේ පළමු සහතික කිරීමේ අධිකාරිය 2009 මැයි 22 දියත් කරන ලදී.

2006 අංක 19 දරන ඉලෙක්ට්‍රොනික ගනුදෙනු පනතට අනුකූලව LankaSign ආයතනය ඩිජිටල් සහතික නිකුත් කිරීමට දැඩි නීති රීති අනුගමනය කිරීමට බැඳී සිටියි. සහතික භාවිතා කරන්නන් සහ ඔවුන්ගේ අදාළ ආයතනවල වලංගුතාවය පිළබඳ කල්තියා හඳුනා ගැනීම, ඩිජිටල් සහතිකයක් නිකුත් කිරීම, වැනි ක්‍රියාවන්හි ඉහළ ආරක්ෂක ප්‍රමිතීන් භාවිතාකිරීම හේතුවෙන් LankaSign හට තොරතුරු ආරක්ෂණ කළමනාකරණ පද්ධති සඳහා වූ අන්තර් ජාතික ISO 27001:2013 සහතිකය ද ලබා ගැනීමට 2015 වර්ෂයේ හැකිවිය. LankaSign විසින් වියදම් ඵලදායි යොදාගැනීමට ඩිජිටල් භාවිතා කිරීම අනෙකුත් සෑම අංශයකම ආයතන දිරිමත් කරයි. ශ්‍රී ලංකාවේ තොරතුරු සුරක්ෂිතතාව ඉහලමට්ටමකින් පවත්වාගනයාම සඳහා ඇති (https://nca.gov.lk) බලයලත් ආයතනය වන Sri Lanka CERT |CC (www.cert.gov.lk) ආයතනය විසින්ද LankaSign CSP (සහතික කිරීම) හි ඉලෙක්ට්‍රොනික සන්නිවේදනය සහ ගනුදෙනු පිළිගෙන ඇත.

1.16 මගේ සංවිධානයට ඩිජිටල් සහතික පද්ධතියක් හඳුන්වා දිය හැක්කේ කෙසේද?

යමෙකු ප්‍රථමයෙන් LankaSign හි මව් සමාගම වන Lanka Clear හා සම්බන්ධ විය යුතුය. (https://www.lankaclear.com) මුල් පිටුවම අවශ්‍ය මඟ පෙන්වීමක් සපයනු ඇත. එහි උපදෙස් අනුව සේවාවන් ලබා ගැනීමට ලියාපදිංචි වන්න. ක්ෂණික ප්‍රතිචාර කවුළුව Pop-Up වෙත පිවිසේන්නේනම් Yes ක්ලික් කිරීමෙන් තොරතුරු මධ්‍යස්ථානය වෙත පිවිස අවශ්‍ය තොරතුරු ලබාගත හැකිය. https://www.lankaclear.com/knowledge-center/lankasign.

1.17 මගේ ලේඛන කළමනාකරණය ස්වයංක්‍රීය කිරීමට හෝ වෙනත් ස්වයංක්‍රිය කාර්ය පටිපාටි සඳහා මට LankaSign ඩිජිටල් සහතික ක්‍රම වේදය භාවිතා කළ හැකිද?

ඔව් ඔබට පුළුවන්. ක්‍රියා පටිපාටියේ විශාල වෙනසක් නැත. මෙහිදී සිදුවන්නේ සාමාන්‍ය ලේඛන වෙනුවට ඩිජිටල් ලෙස අත්සන් කරන ලද ලේඛන ක්‍රියාවලියකට යොමුවීමයි.ඒ සඳහා LankaSign ඩිජිටල් සහතික සහ සාමාන්‍ය මාර්ගෝපදේශ සපයනු ඇත.

1.18 ස්වයංක්‍රීය පද්ධතියක් තුළ නිර්දේශිත ඩිජිටල් සහතික භාවිතය කුමක්ද?

මෙම ඩිජිටල් යෙදුම් තුළ සහතිකර ඇත්නම් ඕනෑම ආකාරයකින් භාවිතා කළ හැකියි. අවශ්‍ය ආයතනයේ අභිමතය පරිදි එය සිදුකෙරේ. එහිදී එම අවශ්‍යතා නීතිමය වැනි සම්මතයන් අභිබවා නොයා යුතුය. මෙම ක්‍රියාවලියට අදාල සහතික සහ අදාළ ධාවක මෘදුකාංග හැර වෙනත් මෘදුකාංග CSP මගින් සපයනු නොලැබේ.

1.19 පාරිභෝගිකයෙකුට ඩිජිටල් සහතිකය ලබා දෙන්නේ කෙසේද?

එය ආරක්ෂිත USB පෝට් එකට බාගත කළ හැකි ලෙස සපයනු ඇත.

1.20 ඩිජිටල් සහතික පද්ධතියක් සැකසීම සඳහා පිරිවැයක් දැරීමට සිදුවේද?

ආරක්ෂක ටෝකනය එක් වරක් මිලදී ගැනීමක් වන අතර ඩිජිටල් සහතිකය වාර්ෂිකව මුදල් ගෙවා අලුත් කරගතයුතුවේ. ආරක්ෂක ටෝකනය සහ ඩිජිටල් සහතිකය පරිශීලක විසින් මිලදී ගත යුතුය මෙම නාමික පිරිවැය හැර, ඩිජිටල් සහතික පද්ධතිය සඳහා වෙනත් ගාස්තු අය නොකෙරේ.

2) තාක්ෂණික තොරතුරු (Technical Information)

2.1 ඩිජිටල් ලෙස අත්සන් කරන ලද ලේඛනයක් ක්‍රියා කරන්නේ කෙසේද?

ඩිජිටල් ලෙස අත්සන් කරන ලද ලේඛනයක් පුද්ගලික අනන්‍ය තාව සහිත උපාංගයක device එකකට පැහැදිලිවම සම්බන්ධ කරයි. එය පුද්ගකික සහ පොදු ප්‍රවේශ දෙකකින් යුත්තයි.

පරිශීලකයාගේ අනන්‍යතාව (උදාහරණයක් ලෙස, ඔවුන්ගේ නම, PIN කේතය, රට, ඊමේල් ලිපිනය, දිනය තහවුරු කර ගැනීමෙන් හා සහතික අධිකාරියේ නම). තහවුරු නොකර වෙනත් කිසිම පාර්ශවයකට මෙම තොරතු වෙත පිවිසිය නොහැක. ඒවා හදුනා ගැනීම සඳහා බ්‍රව්සර් සහ සේවා භාවිතා කරනු ලැබේ.

2.2 PKI (Public Key Infrastructure) යනු කුමක්ද?

PKI යනු ඩිජිටල් සහතික කිරීම් සඳහා ඇති ඩිජිටල් තාක්ෂනය සහ ඊට අදාළ අනෙකුත් යටිතල පහසුකම් සැපීමේ සම්මත ක්‍රියාවලියයි. අද එය අනන්‍ය නොවන අත්සන් සහතික ක්‍රමය ලෙස පිළිගනී. PKI පද්ධතියක, සෑම පරිශීලකයෙකුටම පොදු සහ පුද්ගලික ලෙස ප්‍රවේශ Key දෙකක් ඇත. මෙය ඩිජිටල් ලෙස අත්සන් කරනලද තොරතුරු සහ ඔවුන්ගේ අයිනිකරුගේ සත්‍යතාව තහවුරු කිරීම සඳහා තොරතුරු දත්ත සංකේතනය encrypting කිරීම සහ විකේතනය කිරීම,decrypting සඳහා භාවිතා වේ. පොදු ප්‍රවේශ ඔනමකෙනෙකුට භාවිතා කල හැකි අතර පුද්ගලික ප්‍රවේශ එහි හිමිකරු විසින් ආරක්ෂිතව තබාගනු ඇත. තාක්ෂණිකව මේ දෙක එකිනෙක සම්බන්ද වුවත් පොදු ප්‍රවේශයකින් පවුද්ගලික ප්‍රවේශයකට සම්බන්ද විය නොහැක. මේ අනුව PKI ඩිජිටල් අත්සන් සඳහා වූ විශිෂ්ට තාක්ෂණයක් බවට පත්කර ඇත.

පුද්ගලික ප්‍රවේශ යතුර සාමාන්‍යයෙන් පරිශීලකයාගේ පරිගණක දෘඪ තැටියේ හෝ බාහිර USB ටෝකනයක් වැනි උපාංගයක ගබඩා වේ. පරිශීලකයා පුද්ගලික යතුර පාලනය කරයි. ඒ සඳහම පමණක් නිකුත් කරන ලද මුරපදයක් ඇත. පොදු ප්‍රවේශ යතුර විස්තරාත්මක තොරතුරු සඳහා සංකේතනය කර ඇත. මෙම ප්‍රවේශ වලින් එකක් නොමැති නම් නොගැලපේනම් සත්‍යාපන ක්‍රියාවලිය අසාර්ථක කර ගත නොහැක. මෙයින් අදහස් කරන්නේ සංකේතනය කළ දත්ත විකේතනය කළ නොහැකි බවයි. අනවසර පාර්ශවයන්ට ප්‍රවේශවිය නොහැකි බවයි.

2.3 අපට PKI (Public Key Infrastructure) අවශ්‍ය වන්නේ ඇයි?

ඩිජිටල් සහතිකයේ ප්‍රධාන අරමුණ වන්නේ පොදු ප්‍රවේශ ක්‍රම සහතික කිරීමයි. ඩිජිටල් සහතිකය අයිති වන්නේ සහතිකය නිකුත් කළ ආයතනයට ය, වෙනත් වචනවලින් කිවහොත්, පණිවිඩයක් යවන පුද්ගලයෙකු ඔහු හෝ ඇය කවුද යන්න තහවුරු කර ගැනීමට සහ පසුව යවන්නාට පිළිතුරක් නැවත සංකේතනය කරනලද පණිවිඩ ග්‍රාහකයාට ලබාදීම හැකිවන්නේ ඔවුන්ටයි. ඒ සඳහා පොදු සහ පුද්ගලික ප්‍රවේශ යතුරු භාවිතයේ දී පොදු යතුරු බෙදා හැරීමට සහ හඳුනා ගැනීමට සංකේතාංකන ශිල්පීය ක්‍රම පොදු යතුරු යටිතල පහසුකම් PKI අවශ්‍ය වේ.

2.4 Digital Signature සහ Digital Certificate අතර වෙනස කුමක්ද?

ඩිජිටල් සහතිකයක් යනු පරිශීලකයාගේ සංකේතාත්මක සම්බන්ධතා අනන්‍යතාවය තහවුරු කර උපාංගයක හෝ සක්‍රීය කරන ලද ගොනුවකි.ඩිජිටල් සංඛ්‍යාංක අත්සනක් යනු සත්‍යතාව සැපයීමට සහ අනන්‍යතාවය වලංගු කිරීමට සංඛ්‍යාතන්තු භාවිතා කරන හැෂිං ප්‍රවේශයකි. . ඩිජිටල් අත්සනක් සාමාන්‍යයෙන් රහස්‍ය ප්‍රවේශ යතුරක් භාවිතයෙන් ලේඛනයකට හෝ විද්‍යුත් තැපෑලකට හැෂ්කර ඇති ස්ථාවර වුවකි. අවශ්‍ය විට ලබන්නාට එය ලැබේ, එය පණිවිඩය විවරකිරීම විකේතනය කිරීමdecrypting එම හැෂ් ක්‍රියාවලිය තුලින්ම සිදුවේ. වෙනත් ආකාරයකින් කිවහොත්, ඩිජිටල් සහතිකයක් යනු ඩිජිටල් අත්සනක් සහිත ලේඛනයකි. සහතික කිරීමේ අධිකාරියක් (Certification Authority “CA”) විසින් එය සහතික කර ඇත.

ඩිජිටල් අත්සනක් සහ ඩිජිටල් සහතිකයක් අතර වෙනස පිළිබඳ වැඩි විස්තර:

ඩිජිටල් අත්සන් සහ ඩිජිටල් සහතික (මිනිත්තු 12)
https://www.youtube.com/watch?v=stsWa9A3sOM&t=314s

2.5 සහතික කිරීමේ සේවා සපයන්නෙකුගේ (Certification Service Provider “CSP”) කාර්යභාරය කුමක්ද?

Certification Service Provider “CSP” යනු ආරක්ෂක අක්තපත්‍ර credentials නිකුත් කරන සහ කළමනාකරණය කරන ජාලයගත අධිකාරියකි. ඩිජිටල් සහතිකයක් ලිපිලේඛන පණිවිඩ අත්සන් කිරීම සහ සංකේතනය කිරීම සඳහා පොදු සහ පවුද්ගලික public -private ප්‍රවේශ දෙක යාකරන පොදු ප්‍රවේශයක කොටසක් ලෙස මෙය ක්‍රියා කරයි. තොරතුරු සත්‍යාපනය කිරීම, පරීක්ෂා කිරීම සඳහා CSP ලියාපදිංචි කිරීමේ අධිකාරියක් සමග යටිතල පහසුකම් (PKI), සපයයි. ලියාපදිංචි අධිකාරිය (Registration Authority “RA”)විසින් ඉල්ලුම්කරුගේ තොරතුරු සත්‍යාපනය කරන්නේ නම් සහතිකකිරීමේ අධිකාරියට පසුව භාවිතා කළ හැකි ඩිජිටල් සහතිකයක් නිකුත් කළ හැකිය.

https://www.lankaclear.com/assets/images/knowledge-center/lankasign/downloads/38-CSP-Summary-Certification-Practice-Statement-V3-1.pdf

2.6 LankaSign ඉටු කරන තවත් භූමිකාවන් මොනවාද?

LankaSign සිය පළමු අදියරේදී භාවිතා කිරීම සඳහා බැංකු වෙත ඩිජිටල් සහතික ලබාදීම ආරම්භ කළේය. SLIPS සහ CITS වැනි මූල්‍ය ගනුදෙනු නිෂ්කාශන පද්ධති (චෙක් පරික්ෂාව සහ ගනුදෙනු) පාරිබෝගික ආරක්ෂණ ක්‍රම CSP සහ පොදු ප්‍රවේශ Public Key Infrastructure (PKI) පහසුකම් මෙන්ම පුද්ගලික වීර්චුඅල් ජාල LCPL's Virtual Private Network (VPN) ස්ථාපිත කර ඇත. 2011 පෙබරවාරි 9 වන දින LankaSign විසින් ඩිජිටල් සැපයීමේ දෙවන අදියර දියත් කරන ලදී. එමගින් සියලුම මූල්‍ය අංශයේ ව්‍යවසාය යෙදුම් සඳහා සහතික, SSL සහතික සහ අවසාන පරිශීලකයන් (ඊමේල්/ලේඛන අත්සන්

කිරීමේ සහතික) පුද්ගලික සහ පොදු ජාල දෙකෙහිම සම්බන්ද කර ඇත. LankaSign හි ඩිජිටල් සහතික භාවිතා කිරීම නිසා ශ්‍රී ලංකාවේ මූල්‍ය අංශයට විශාල වටිනාකමක් හිමිවී තිබේ.

එමගින් රටේ වටිනා විදේශ විනිමය ඉතිරි කර දෙනු ඇත. පාරිභෝගික ආරක්ෂණ පද්ධති කිසා CSP විදේශ වලින් සහතික මිලක් ලබාගැනීමටද හැකිවේ. LankaSign භෞතික ලේඛන කළමනාකරණය හා සම්බන්ධ ලේඛන කළමනාකරණ පොදු කාර්ය,හරිත මූලාරම්භයන් ප්‍රවර්ධනය කිරීම මෙන්ම.ව්‍යාප්තිය,මගින් පාරිභෝගික කේන්ද්‍රීය දේශීය සේවාවක් සහවිදේශීය සේවාවන් සදහා අඩු කිරීමට විසඳුම් සපයයි.

Lanka Sing ආයතනය දියත්කර ඇති ඩිජිටල් අත්සන් කිරීම මෙන්ම ඔවුන්ගේ ස්වයංක්‍රිය ලේඛන ක්‍රියාවලිය තවත් අංශ කිහිපකින් සමග මූල්‍ය ආයතන රැසක බහුලව භාවිතා වේ. ලේඛනවල ඉලෙක්ට්‍රොනික පිටපත් සහ විද්‍යුත් ලියකියවිලි සඳහා ඉහළ ආරක්ෂාවක් එක් කිරීම හුවමාරු ක්‍රියාවලිය ඒ අතරවේ. ඔවුන්ගේ පුළුල් කිරීමේ සැලැස්මේ මීළඟ අදියර ලෙස, ප්‍රධාන උත්ශ්‍රේණිගත කිරීමක් සමඟ එමමොහොතේම real -time ජංගම දුර කථන පදනම් කර ගනිමින් ඩිජිටල් ලෙස අත්සන් කිරීම සහ ඉලෙක්ට්‍රොනික සත්‍යාපනය සිදුවනු ඇත. LankaSign විසින් වැඩි දියුණු කරන ලද පොදු API එකක් මගින් මෙය සක්‍රීය කර ඇත. මෘදුකාංගයක් හරහා එවැනි ජංගම ගෙවීම් යෙදුම් සමඟ පහසුවෙන් ඒකාබද්ධ කළ හැක. වැඩසටහන් සම්පාදකයන් සදහා මේ නොමිලේ බෙදා හරිනු ඇත.

සියලු වැඩිදුර විමසීම් යොමු කරන්න:
චානුක වත්තේගම

අධ්‍යක්ෂ - ප්‍රතිපත්ති,
ශ්‍රී ලංකා තොරතුරු හා සන්නිවේදන තාක්ෂණ නියෝජිතායතනය
විද්‍යුත් තැපෑල - chanukaw@icta.lk